NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

AN INTEGRATED INTRANET AND DYNAMIC DATABASE APPLICATION FOR THE SECURITY MANAGER AT NAVAL POSTGRADUATE SCHOOL

by

Sonja Michele Perry

September 2002

Thesis Advisor: Randy L. Borchardt
Co-Advisor: Dan C. Boger

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	September 2002	Master's Thesis

4. TITLE AND SUBTITLE An INTEGRATED INTRANET AND DYNAMIC DATABASE APPLICATION FOR THE SECURITY MANAGER AT NAVAL POSTGRADUATE SCHOOL

5. FUNDING NUMBERS

6. AUTHOR (S) Name Sonja Michele Perry

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the U.S. Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words) **This thesis presents an analysis, design and implementation of the Naval Postgraduate School's Sensitive Compartmented Information Facility (SCIF) consolidated Access database and website. The database was designed using a Microsoft Access 2000 relational database. This new database consolidates two previously separate personnel and classified inventories databases. The SCIF website was created utilizing Macromedia's Dreamweaver MX. Active Server Pages are used to provide connectivity between the website and database. The website accessible via any standard browser will provide the capability for designated users to manipulate data in the database. Protection of sensitive data is implemented utilizing Macromedia's embedded user authentication features.**

14. SUBJECT TERMS DATABASES, INTRANET, ACCESS 2000, MACROMEDIA, DREAMWEAVER

15. NUMBER OF PAGES 85

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500 **Standard Form 298 (Rev. 2-89)**
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited.

An INTEGRATED INTRANET AND DYNAMIC DATABASE APPLICATION FOR THE SECURITY MANAGER AT NAVAL POSTGRADUATE SCHOOL

Sonja Michele Perry
Lieutenant, United States Navy
Criminal Justice B.S., Old Dominion University, 1993

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIECE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL

September 2002

Author: Sonja Michele Perry

Approved by: Randy L. Borchardt, Advisor

Dan C. Boger, Co-Advisor

Dan C. Boger, Chairman
Information Sciences Department

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis presents an analysis, design and implementation of the Naval Postgraduate School's Sensitive Compartmented Information Facility (SCIF) consolidated Access database and website. The database was designed using a Microsoft Access 2000 relational database. This new database consolidates two previously separate personnel and classified inventories databases. The SCIF website was created utilizing Macromedia's Dreamweaver MX. Active Server Pages are used to provide connectivity between the website and database. The website accessible via any standard browser will provide the capability for designated users to manipulate data in the database. Protection of sensitive data is implemented utilizing Macromedia's embedded user authentication features.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION 1

A. BACKGROUND 1

B. PURPOSE 2

C. SCOPE AND ORGANIZATION OF STUDY 3

1. Process 3

2. Design 3

3. Import Data 4

4. Prototype 4

5. Front-end/Back-end 4

6. Documentation 4

D. CHAPTERS 4

II. DATABASE DEFINITION AND DESIGN 7

A. MICROSOFT ACCESS 2000 7

1. New Features 7

2. Security 8

3. System Requirements 8

4. Access Objects 8

a. Data Organization 9

b. Supporting Functions 10

B. THE RELATIONAL DATABASE MANAGEMENT SYSTEM (RDMS) . 11

C. JOIN PROPERTIES 12

D. REFERENTIAL INTEGRITY 13

E. KEYS 14

F. NORMALIZATION 14

1. First Normal Form (1NF) 15

2. Second Normal Form (2NF) 15

3. Third Normal Form (3NF) 15

4. Fourth Normal Form (4NF) 15

5. Fifth Normal Form (5NF) 16

III. SCIF DATABASE REQUIREMENTS AND DESIGN 17
A. SCIF ENTITIES 17
B. SCIF ENTITY RELATIONSHIP DIAGRAM 24
C. NPS SCIF DATABASE FORMS 25
IV. INTRANET AND DATABASE CONNECTIVITY 31
A. DREAMWEAVER MX 31
B. SCIF SITE DESIGN 31
1. Login Page 33
2. Homepage 33
3. Form Choice Page 34
4. Data Detail Page 35
5. Data Insert Page 36
6. Data Delete Page 37
7. Personnel Detail Form 38
8. Personnel Update Form 39
9. Personnel Delete Form 40
C. DREAMWEAVER USER SECURITY 41
1. Administrator Group 42
2. Limited Administrator 42
3. Extended User 42
4. User 43
D. DREAMWEAVER SITE SECURITY 43
V. SUMMARY 45
APPENDIX I ADMINISTRATOR USER MANUAL 47
LIST OF REFERENCES 65
BIBLIOGRAPHY 67
INITIAL DISTRIBUTION LIST 69

LIST OF FIGURES

Figure 1. The Basic and Supporting Functions of Access (After:[1]) 9
Figure 2. SCIF Entity Relationship Diagram 24
Figure 3. Start-up form 25
Figure 4. Data Form 26
Figure 5. SCIF Personnel Account Form 27
Figure 6. Personnel Access Level Form 28
Figure 7. Personnel Subcustody Form 29
Figure 8. Personnel Comments Form 30
Figure 9. SCIF Website Conceptual design 32
Figure 10. Login Page 33
Figure 11. SCIF homepage 34
Figure 12. Form Choice Page 35
Figure 13. Data Detail Page 36
Figure 14. Data Insert Form 37
Figure 15. Data Delete Form 38
Figure 16. Personnel Detail Form 39
Figure 17. Personnel Update Form 40
Figure 18. Personnel Delete Form 41

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. SCIF Entities 18
Table 2. Personnel Entity 19
Table 3. Data Entity 21
Table 4. Personnel_Data Entity 21
Table 5. Access Entity 22
Table 6. Additional Tables 23
Table 7. Website Authorization Table 44

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGEMENTS

I’d like to thank all the people that helped me complete this thesis. Specifically I’d like to thank my thesis advisors Randy Borchardt and Dan Boger, the Special Security Officer, Andy Andersen and staff.

To Albert and Barbara Ballard, thanks for a wonderful place to live while completing my thesis work. I will forever remember the scenic views of the Monterey Bay.

A special thanks to all the friends and family that have supported me both in graduate school and throughout my Naval Career.

And last, I dedicate this thesis to my Dad, who I’ll call my silent supporter, and my Mom, the vocal one. Mom, your support and guidance means everything to me. You are the best friend and mother a person could want. Because of all of you I feel blessed in so many ways.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

The Naval Postgraduate School (NPS) Security Manager/Special Security Officer (SSO), as part of his overall responsibilities to safeguard classified information, maintains up-to-date, accurate personnel and classified material inventories. To aid accomplishment of these tasks, the NPS Security Manager had attempted to develop two separate flat-file databases using Access 95/97 to track mission-critical information.

These databases, while minimally acceptable in the past to simply track personnel and classified material, are obsolete and no longer fully support the staff's expanding information needs. As designed, these database systems do not interface with each other, requiring the use of two separate applications and duplicate data entry by database maintainers. For reasons unknown to the SSO staff, the existing materials database is not functioning properly and data corruption is suspected as database modify controls were enabled for both database users and maintainers. Additionally, since the databases were placed into the production environment, several new business practices have evolved, requiring a more versatile and robust database.

A functional relational database would reduce redundant data entry requirements, ease user interaction with the large amounts of data involved, and improve customer service and accountability. As Microsoft 2000 products are in widespread use at the Naval Postgraduate

School, the front-end of the Sensitive Compartmented Information Facility (SCIF) database will be an Access 2000 project.

B. PURPOSE

The purpose of this research is to provide an integrated intranet and dynamic access database application for the Security Manager that:

1. Implements user-level security to prevent unauthorized access to SCIF information.

2. Combines functionality of two existing databases with additional features required by the end-users into one consolidated user-friendly application.

3. Store the database on a server to enable multiple user access.

The objectives of this thesis are:

1. To develop and design a consolidated Access 2000 Database for the personnel and classified material inventories.

2. To allow users access to Security Manager specified information on the Classified Intranet via any standard web browser (i.e., Internet Explorer).

3. To provide a user-friendly front-end interface, allowing users with limited computer skills to retrieve information as needed.

4. To provide comprehensive documentation that allows any database-savvy administrator to make modifications allowing for future database upgrades.

5. To address database security issues by implementing user-level security and permission settings.

C. SCOPE AND ORGANIZATION OF STUDY

The scope of thesis included the following:

1. Process

A comprehensive requirements analysis for the proposed database was conducted. The primary requirement generation method used included conducting ongoing interviews with stakeholders concerning desirable changes and inclusions for the new and improved database.

2. Design

During the design phase, new database templates that combine current information requirements with capabilities desired by the stakeholders were developed. Access and Dreamweaver forms provide the interface to information in the SCIF database.

3. Import Data

The new database was populated by importing the existing database data into the new database system after the integrity of the data was verified.

4. Prototype

Two phases were used to prototype the database. A standalone version of the new database was developed and tested using Access 2000. The second phase consisted of testing the prototype database using a front-end and back-end.

5. Front-end/Back-end

Following an evaluation period of the stand-alone prototype, the Access database was connected to a front-end intranet web site.

6. Documentation

The model, including the design and implementation of the SCIF relational database, was documented.

D. CHAPTERS

This thesis is organized as follows:

- Chapter I Introduction – provides a brief description of the objectives of the thesis, the scope, organization and methodology of study.

- Chapter II Access 2000 Definition and Design - is a detailed description of the Access database concepts and design.
- Chapter III Access 2000 Project – is detailed description of the Access database project.
- Chapter IV Intranet and Database Connectivity – describes how the database will be accessible via the classified intranet.
- Chapter V Summary – This chapter provides a short summary of the thesis and addresses possible future modifications.
- Appendix I – User’s Manual.

THIS PAGE INTENTIONALLY LEFT BLANK

II. DATABASE DEFINITION AND DESIGN

This chapter will explain the defining characteristics of relational database systems. Specifically, this chapter will address Microsoft Access 2000 concepts used in creating the SCIF database. Topics covered will include referential integrity, primary and secondary keys, normalization and join properties.

A. MICROSOFT ACCESS 2000

Microsoft Access 2000 is a powerful and robust 32-bit relational database management system used for creating desktop and client/server database applications. Access 2000 is a part of the Microsoft Office 2000 Professional and Developer editions.

1. New Features

There have been several changes from Access 97 to Access 2000. The most significant change is the adoption of ActiveX Data Objects (ADO) 2.1, which replaces Data Access Objects (DAO) embedded in previous Access versions. While still supporting databases using DAO, the future of data and database connectivity for Office will be based on ADO, making DAO obsolete in the long term. In the past Access used macros for programming. Access 2000 continues to use macros; however, Microsoft recommends that database designer’s start transitioning to Visual Basic for Applications (VBA) 6.0 as macros may not be supported in

future versions of Access. Access 2000 offers Internet-related features for creating HTML documents for use on intranets and the Internet. Perhaps the most important improvement in Access 2000 is the addition of Data Access Pages (DAP) which allow the display of static web pages. [1]

2. Security

Access is designed for creating applications for multiple users. Access has a security system that prevents unauthorized persons from viewing or modifying database files shared on networks. Access 2000 inherits security features from Microsoft’s SQL Server. [1]

3. System Requirements

Access 2000 is a resource-intensive application as are all Office 2000 software packages. Office 2000 requires a Pentium PC with a minimum of 32 MB of RAM, Windows 95/98/NT v4.0/2000 and a minimum of 400MB of free space. [1]

4. Access Objects

A full scale Access application includes various types of objects. Access table, form, report and query objects serve the four basic functions of Access that organize data in an application structure.

a. Data Organization

Good database design requires the use of a top-down sequence. Tables are created first; queries based on those tables are created next; and finally forms and reports are created using queries. Figure 1 shows the basic organization in sequence. [1]

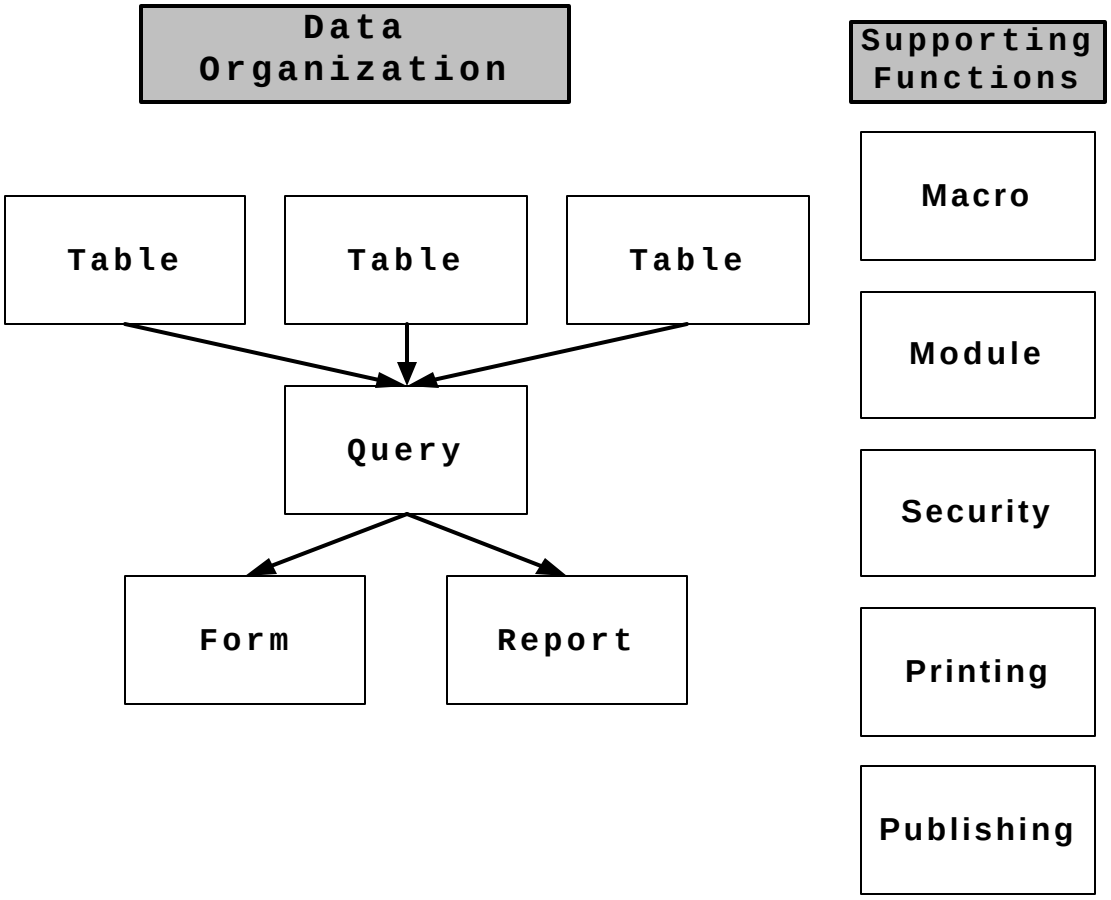


Figure 1. The Basic and Supporting Functions of Access (After:[1])

- Table – An object that stores information added to the database by the user. Forms are the medium used for data entry. [1]
- Query - An object that allows filtering, sorting and combining of data. Good database design dictates forms and reports be based on queries. [1]
- Forms – An object used to enter and view data in the database. A form presents data in logical format. Forms are user friendly and the use of format controls ensures correct data entry via dropdown boxes and validation rules. [1]
- Reports - Allow the printing of detailed, summary information from both queries and tables. The ability to provide meaningful reports is one of the defining purposes of a database. [1]

b. Supporting Functions

Supporting functions provide the database with additional options that improve functionality exponentially.

- Macro – A sequence of actions that automates repetitive database operations. [1]
- Modules – Functions and procedures written in the Visual Basic for Applications (VBA) programming language. The capabilities of modules exceed those of standard macro actions. Modules will

eventually replace macros in future releases of Access. [1]

- Security – Allows granting access and permissions to users or groups, restricting their ability to view or modify all or a portion of the tables in the database. [1]
- Printing – Allows virtually anything viewed in Access's run mode to be printed.[1]
- Publishing - Allows publishing of World Wide Web (WWW) pages using Data Access Pages (DAP). [1]

B. THE RELATIONAL DATABASE MANAGEMENT SYSTEM (RDMS)

An RDMS is an application that can create, organize and edit information. The information may be displayed through user or designer selected views and printed in formatted reports. Most RDMSs include macro functionality or a macro language. Access, a desktop RDMS, uses the programming language Visual Basic for Applications.

One of the advantages of a RDMS is the ability to use multiple relationships between tables that store data. Multiple relationships overcome inherent storage inefficiencies created when all information is placed in a single table and improve database effectiveness. A unique identification number is required for each record entered into a table. This identification (ID) number is usually assigned automatically by the database and serves as the primary key when in its parent table and as a foreign key when it is in an associated table. Association of the two

tables using primary and foreign keys creates a relationship.

Relationships between tables can exist in four forms:[1]

1. **One-to-one relationships**: In a one-to-one relationship, a record from the primary table is related to only one record in the associated table.

2. **One-to-many relationship**: In a one-to-many relationship, a record in the primary table may have many related records in the second table, but for any record in the second table, there is only one matching record in the first table. This is the most common of the relationship types.

3. **Many-to-one relationship**: A many-to-one relationship is much the same as a one-to-many relationship, only viewed from the opposite vantage point.

4. **Many-to-many relationships**: A many-to-many relationship occurs when there are no unique relationships between tables. This type of relationship is resolved by making an intermediate table that connects two one-to-many relationships.

C. JOIN PROPERTIES

A join is the process of linking tables or queries by associating data fields in the tables or query. The default field for association is the primary key field in one table to those that have the same key field in the associated table.

There are four types of joins in a database. [1]

1. **Equi-join (inner joins)**: The equi-join is the most common type of join. This type of join returns only values from both tables.

2. **Outer join**: A join that returns all rows from one of the tables even if there are no matching values from the other table.

3. **Theta join**: A join that allows relating data by using comparison operators other than the equal sign (=) are named Theta joins. Theta joins are created by using the less than (<) or greater than (>) signs.

4. **Self-join**: A self-join relates data parameters within a single table.

D. REFERENTIAL INTEGRITY

Referential integrity is probably the most important feature in database design that is available in all versions of Access. Referential integrity prevents the creation of records without connection to a primary table. Referential integrity enforcement prevents deletion or modifications of data in a parent table (the one side in a one-to-many relationship) on which data from child table (the many side in a one-to-many relationship) depend. Two update features help maintain referential integrity: cascading updates and cascading deletions. The cascading update feature automatically updates all known associations after a record is changed in the database. Cascade delete,

after deletion of a record, deletes any associated records. [2] As such, the cascade delete function should be used with care as it may cause unintentional loss of data and corruption of the database.

E. KEYS

Each table in a database must have a key assigned. A key uniquely identifies a row. There are two types of keys: primary and foreign. A primary key is a field that uniquely identifies a record. A foreign key is the primary key from one table inserted into another table in the database. The primary key can be based on more than one field in the record; for instance, a primary key may include a foreign key and one or more fields in the record.

F. NORMALIZATION

Normalization is the process of evaluating and converting a relation to reduce the number of modification anomalies. An anomaly is an undesired consequence of data modification. The purposes of normalization include the following [3]:

- Elimination of duplicate information in tables.
- Accommodation of future changes in the structure of tables.
- Minimization of database structural change on user applications that utilize the data.

1. First Normal Form (1NF)

First normal form requires that a table contain no repeating groups and that data cells contain only one value. It also requires that all columns in a relational database table be unique. Any table that contains duplicate data must be separated into two separate tables to satisfy first normal form criteria.

2. Second Normal Form (2NF)

Second normal form requires that all non-key columns be fully dependent on the primary key, which requires each column to be determined by the primary key. A table must be in first normal form before applying second normal form rules. Second normal form will reduce redundancy errors associated with the first normal form criteria.

3. Third Normal Form (3NF)

Third normal form requires that tables conform to both first and second normal forms. It also requires that all non-key columns be dependant on the table’s primary key and independent of each other (i.e., no transitive dependencies). Third normal form eliminates most of the anomalies known in databases today and is the most common standard for normalization in commercial databases.

4. Fourth Normal Form (4NF)

Fourth normal form is a unique type of normalization that pertains to tables when many-to-many relationships

occur requiring that independent data entries be stored in the same table. A table is in fourth normal form when all multi-valued dependencies have been eliminated.

5. Fifth Normal Form (5NF)

Fifth normal form requires compliance with the rules of third normal form and fourth normal form when many-to-many relationships exist. Fifth normal form requires reconstruction of the original table from previously separated tables to achieve normal form requirements.

III. SCIF DATABASE REQUIREMENTS AND DESIGN

The SCIF database is designed to meet certain requirements. First the database must be able to store relevant information on personnel and classified libraries data. Second, the SCIF database will be intranet accessible via any standard web browser. Third, access to database information must be secured by implementing four access levels:

- The normal user will be able to view only the classified inventory. This is most restrictive access level.
- The extended user will have read privileges for both the personnel and data portions of the database.
- The limited administrator will have full read/write access to the data contained in the database.
- The administrator is the least restrictive access level. The administrator will have full access and control over the database, including the ability to modify the database schema.

A. SCIF ENTITIES

There are four entities in the SCIF database. The following, Table 1, lists the four entities embedded in the security manager relational database; the table also

provides a brief description of each table’s associated business rule.

Entity	Business Rules
Personnel	Information concerning personnel entered into the database
Data	Information concerning materials entered into the database
Personnel_ Data	Contains information regarding personnel that have custody of data
Access Level of Personnel	Contains personnel access level related information

Table 1. SCIF Entities

The personnel table below, Table 2, contains descriptive information about each attribute in the personnel table.

PERSONNEL	**Data Type**	**Description**
PersonnelID	AutoNumber	A unique identification number assigned by Access to each person
LastName	Text	Last Name
FirstName	Text	First Name
SSN	Text	Social Security Number
Phone	Text	Telephone Number
Bldg#	Text	Building Number
Room#	Text	Room Number
SIPRNETID	Text	Secret Internet Identification
SIPRNETEMAIL	Text	Secret Internet Email Address
NSANETID	Text	National Security Agency Internet Identification
NSANETEMAIL	Text	National Security Agency Internet Email Address
UNIXID	Text	(UNIX) Identification
UNIXEMAIL	Text	UNIX Email Address
JDISSID	Text	Joint Deployable Information Security System (JDISS) Identification
JDISSEMAIL	Text	Joint Deployable Information Security System Email

Table 2. Personnel Entity

The data entity, Table 3, contains descriptive information about each attribute in the data table.

Data	Data Type	Description
DataID	AutoNumber	A unique identification number assigned by Access to each piece of data
BarCode#	Text	A unique identification number assigned by Access to each person
Classification	Text	Barcode number of the piece of material
Originator	Text	Originator of Material
DIA Production#	Text	DIA Production number of material
Copy#	Number	Copy# of material
DateofMaterial	Date/Time	Date material created
Subject	Text	Subject of material
Date Received	Date/Time	Date material received at the command
Abstract	Text	Brief overview of material
MediaTypeID	Text	Type of media the material is contained in
LastUpdate	Date/Time	Date of last update
Destroyed	YES/NO	Material destroyed (Yes/No)
DateDestroyed	Date/Time	Date material destroyed
Destroyedby	Text	The person destroying the material
Witnessedby	Text	The person witnessing the destruction of the material

Authorizing Person	Text	The person authorizing the destruction or transfer of the material
Safe#	Number	Safe# where the material is stored
Drawer#	Number	Drawer# where the material is stored
CheckOutDate	Date	Date material checked out
CheckInDate	Date	Date material checked in
Other	Text	Other pertinent information

Table 3. Data Entity

Table 4, the Personnel_Data table contains the PersonnelID and DataID primary keys. The Personnel_Data joins the personnel table to the data table.

Personnel_Data	**Data Type**	**Description**
PersonnelID	Number	A unique identification number assigned by Access to each person
DataID	Number	A unique identification number assigned by Access to each piece of data

Table 4. Personnel_Data Entity

The access table contains descriptive information about each person and their associated access levels.

Access	Data Type	Description
AccessID	AutoNumber	A unique identification number assigned by Access to each person
PersonnelID (FK)	Number	A unique identification number assigned by Access to each person
Level	Checkbox	Access level of personnel. a choice of SI, TK, BYE, GG, EU, or NK

Table 5. Access Entity

The additional tables contain information about the database’s lookup tables, destroyed data tables and sub-custody tables.

Additional Tables	**Description**
Safe Lookup	Safe numbers in SCIF
Drawer Lookup	Drawer numbers in safe
Media Type Lookup	Dropdown menu with a choice of CD, DVD, Floppy Disk, Publication, Video, Working Papers or Zip Disk
Authorization Lookup	List of personnel with destruction authorization.
Destroyed Data	Table of destroyed data
Subcustody Data	Table of data that is checked out to personnel

Table 6. Additional Tables

B. SCIF ENTITY RELATIONSHIP DIAGRAM

Figure 2 shows the four tables and associated attributes in the SCIF database. It displays the three one-to-many relationships that connect the four tables together and associated lookup tables. The Personnel and Access Level of Personnel is a one-to-many relationship. The one-to-many relationship states that personnel can have more that one access level. By design, the Personnel and Access Level one-to-many relationship enforces referential integrity by selecting the cascade update of related fields and cascade delete of related records. The database is designed in this manner so that when a person is deleted from the database, the associated access levels are also

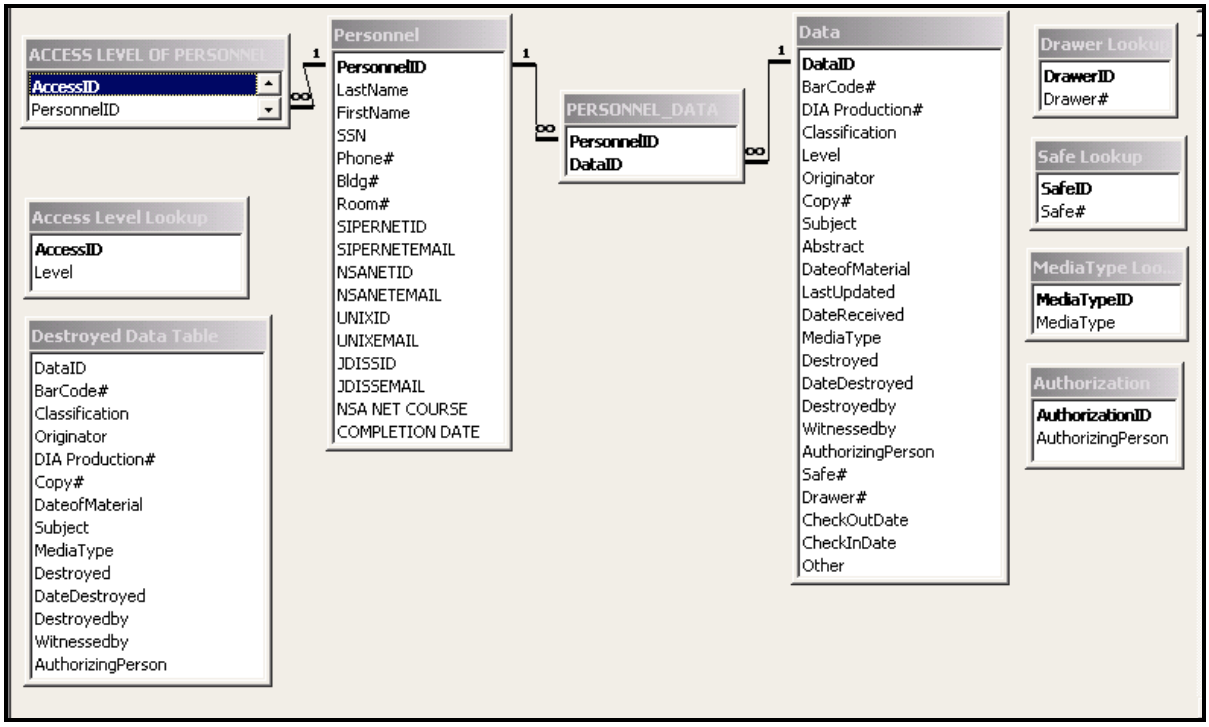


Figure 2. SCIF Entity Relationship Diagram

deleted from database tables and queries. The Personnel and Data tables have a many-to-many relationship. The Personnel_Data table is the intermediate table that connects two one-to-many relationships. Enforcement of referential integrity for this many-to-many relationship will allow the cascade update of related fields. The cascade delete of related records is not selected for the personnel-data relationship for two reasons. First, it alerts the database maintainer that the person to be deleted has not returned classified data checked out from the library. Second, it forces the database maintainer to place the data back into the SCI library circulation, allowing other users possible access to that data.

C. NPS SCIF DATABASE FORMS

The first form that a user will see is the SCIF startup form displayed in Figure 3.

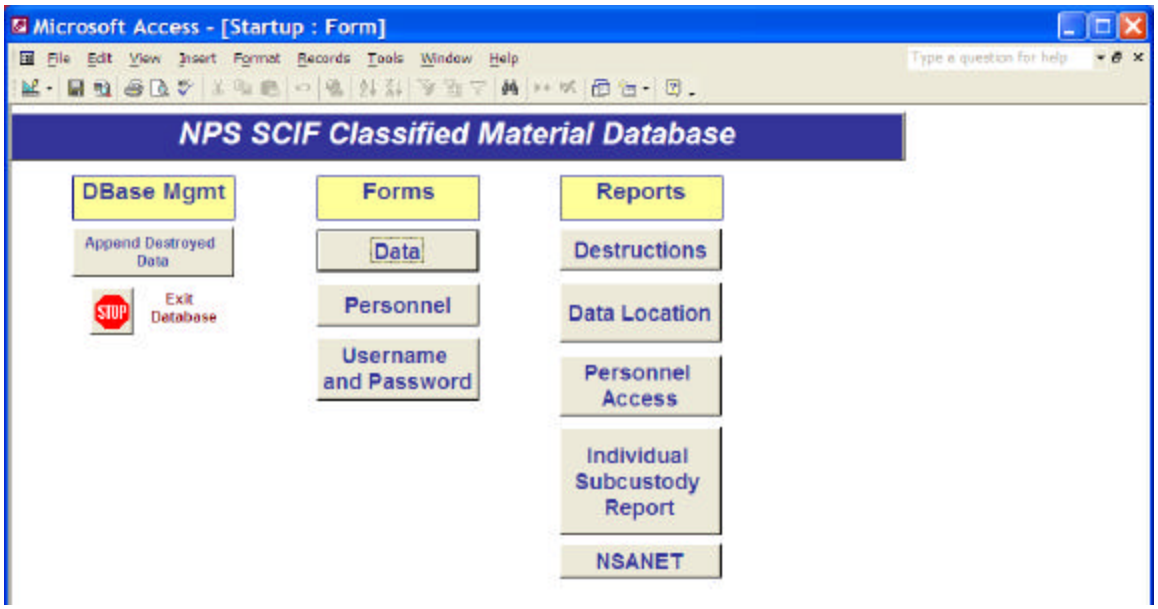


Figure 3. Start-up form

It has three headings: database management, forms and reports. Located underneath the database management (Dbase Mgmt) heading is an action button to append destroyed data from the active database into a destroyed data table. The purpose of the destroyed data table is to maintain an archive of all data that has been destroyed.

Below the forms heading there are data, personnel, username and password action buttons to enter related information. Under the reports heading there are action buttons to print destruction information, data location, personnel access, subcustody reports, and NSANET related data.

The data form, shown in Figure 4, allows the user to enter all data related information into the SCIF database. It also allows the user to enter destruction-related information.

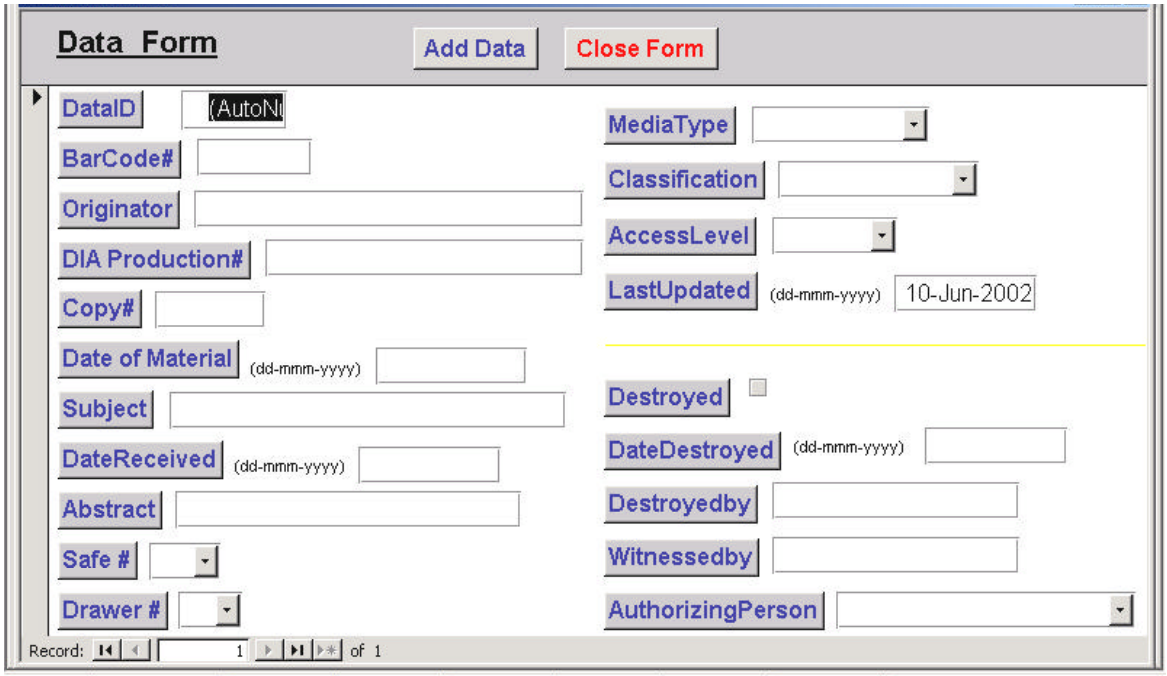


Figure 4. Data Form

The personnel form, shown in Figure 5, allows the user to enter data about people stationed at the Naval Postgraduate School. This form has a main form, which contains personnel general data, and four tabbed sub-forms that contain data related to each person. The first sub-form documents NSANET, UNIX, SIPRNET and JDISS account related information.

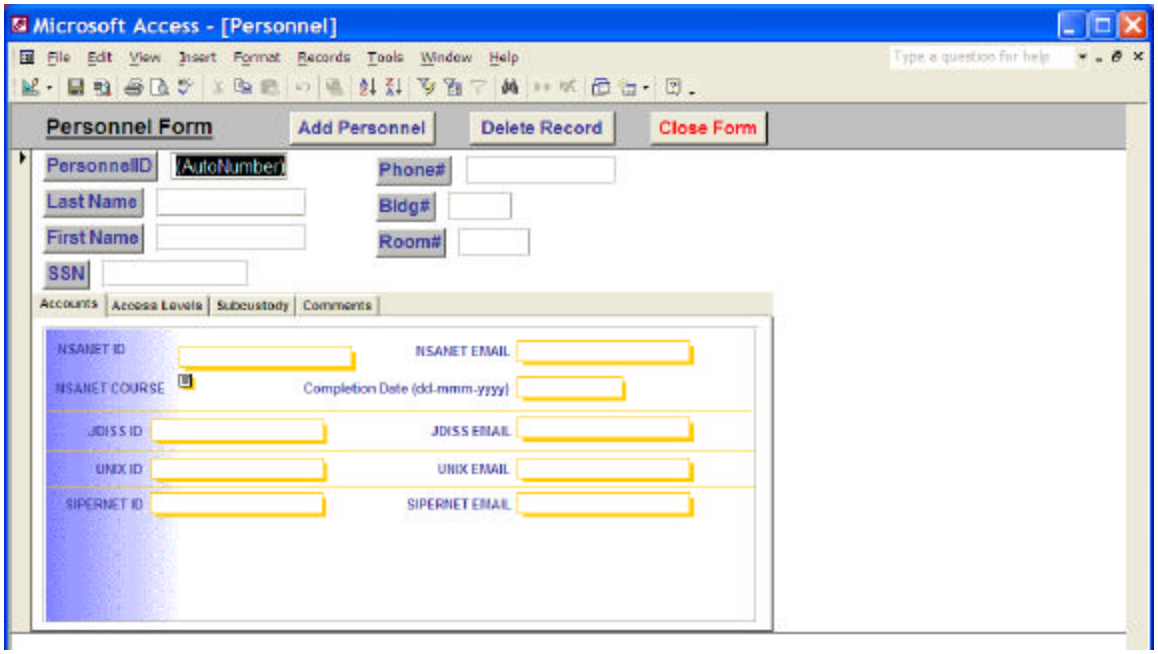


Figure 5. SCIF Personnel Account Form

Figure 6 depicts the personnel form with the second subform which documents the various access levels of each person.

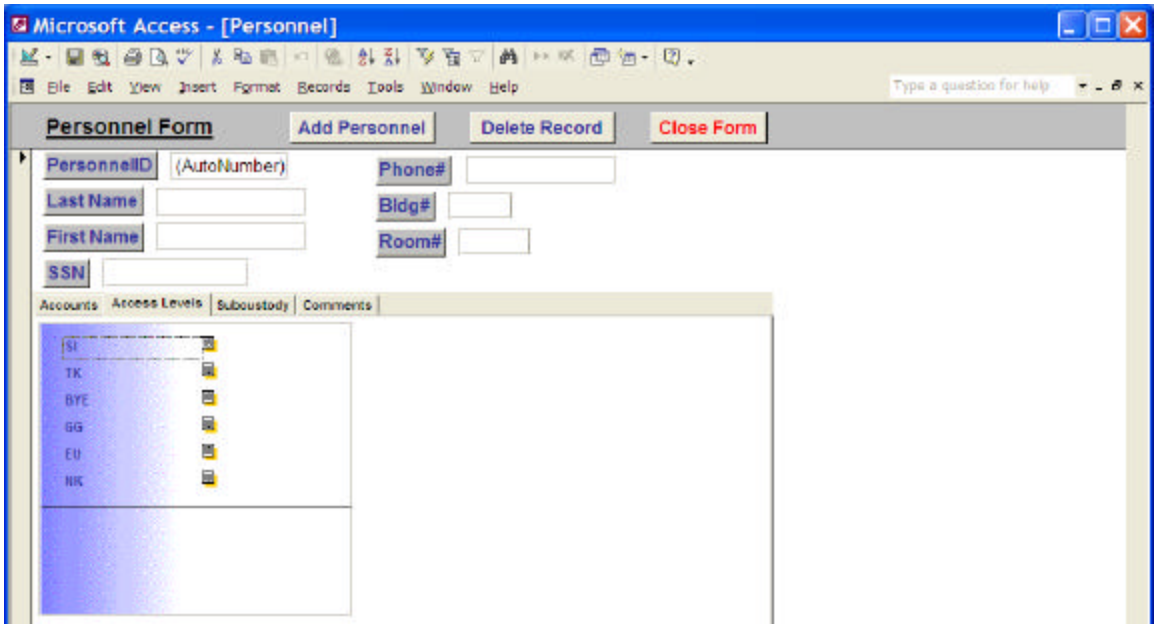


Figure 6. Personnel Access Level Form

Figure 7 depicts the personnel subcustody form and shows relevant classified data custody information. This form is used to check classified documents out to personnel. The DataID field is a dropdown menu that will display information available for checkout. Once the item is selected the associated Barcode, Subject and Classification fields will automatically update.

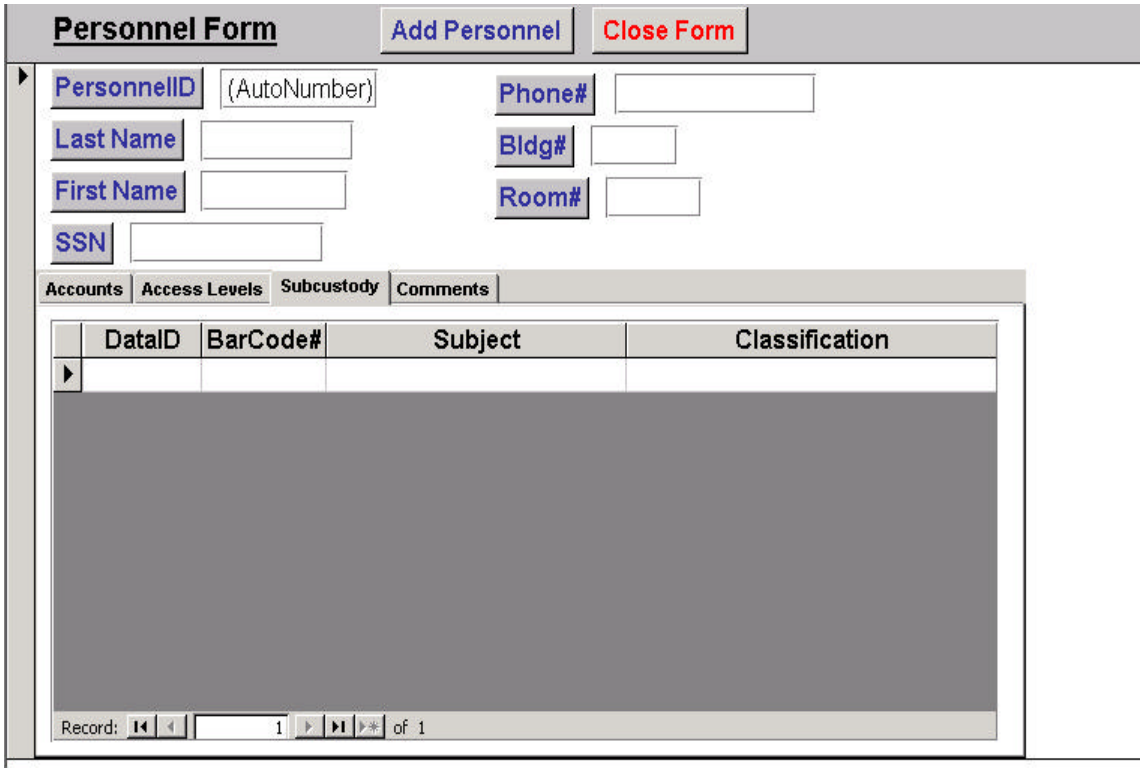


Figure 7. Personnel Subcustody Form

Figure 8 depicts the comment sub-form. This form inserts a general comment subform, which allows a user to enter any other pertinent information.

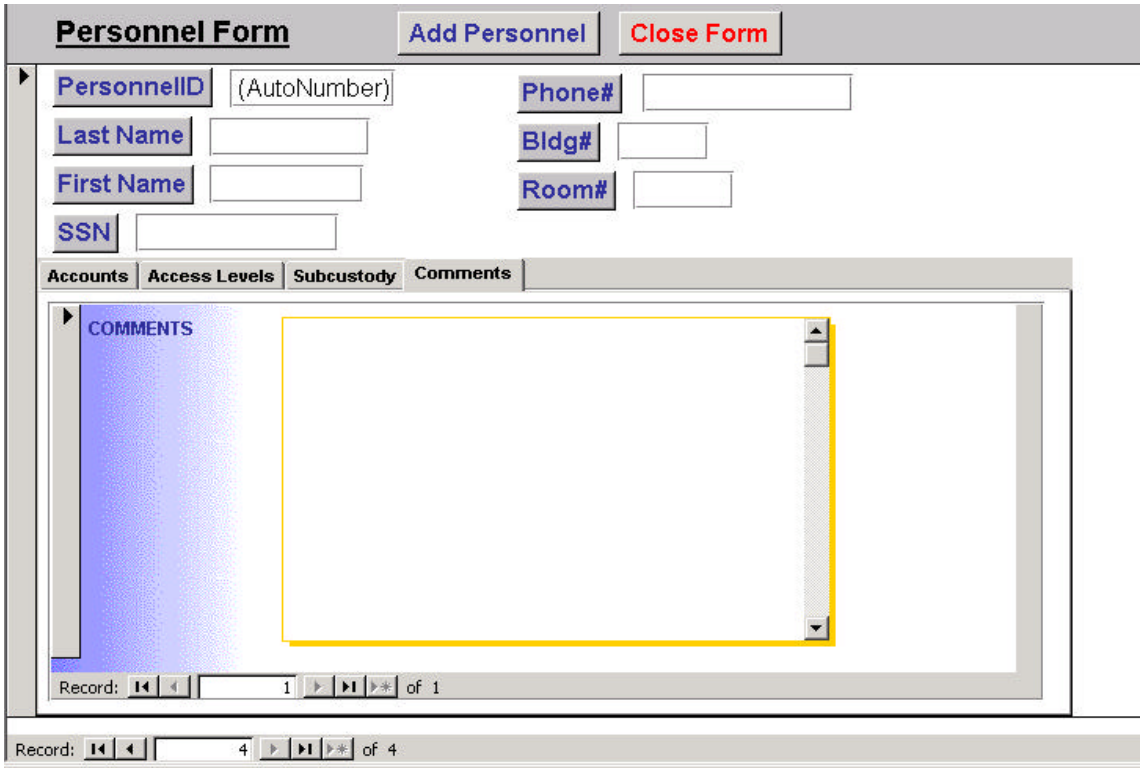


Figure 8. Personnel Comments Form

IV. INTRANET AND DATABASE CONNECTIVITY

This chapter describes how the intranet website is designed and how the site will access the SCIF database.

A. DREAMWEAVER MX

Dreamweaver is a web design application that uses WYSISWYG (what you see is what you get) design tools and a powerful HTML text editor.[4] The application's WYSISWYG assists in webpage development by automatically generating HTML code for application-defined routine procedures while simultaneously allowing the web designer to add code to customize webpage development. One of the main advantages of using Dreamweaver for web page development is that it greatly reduces manual coding for designers. However, an elementary level of knowledge is still required to aid in trouble shooting errors in Dreamweaver generated code. Roundtrip HTML is another unique and useful feature of Dreamweaver. This feature allows Dreamweaver to open any HTML page created in any other program without any alteration to the page.[4]

B. SCIF SITE DESIGN

Figure 9 displays the web site architecture. The site's homepage is index.htm. All web file names will be entirely in lower case to ensure that they will load correctly on various platforms. From the homepage the user can decide to enter either the form or report choice

portion of the site. All users will be able to see the data detail form and the classified inventory report. Access to the other pages will be controlled based on the user's authorizations and access level.

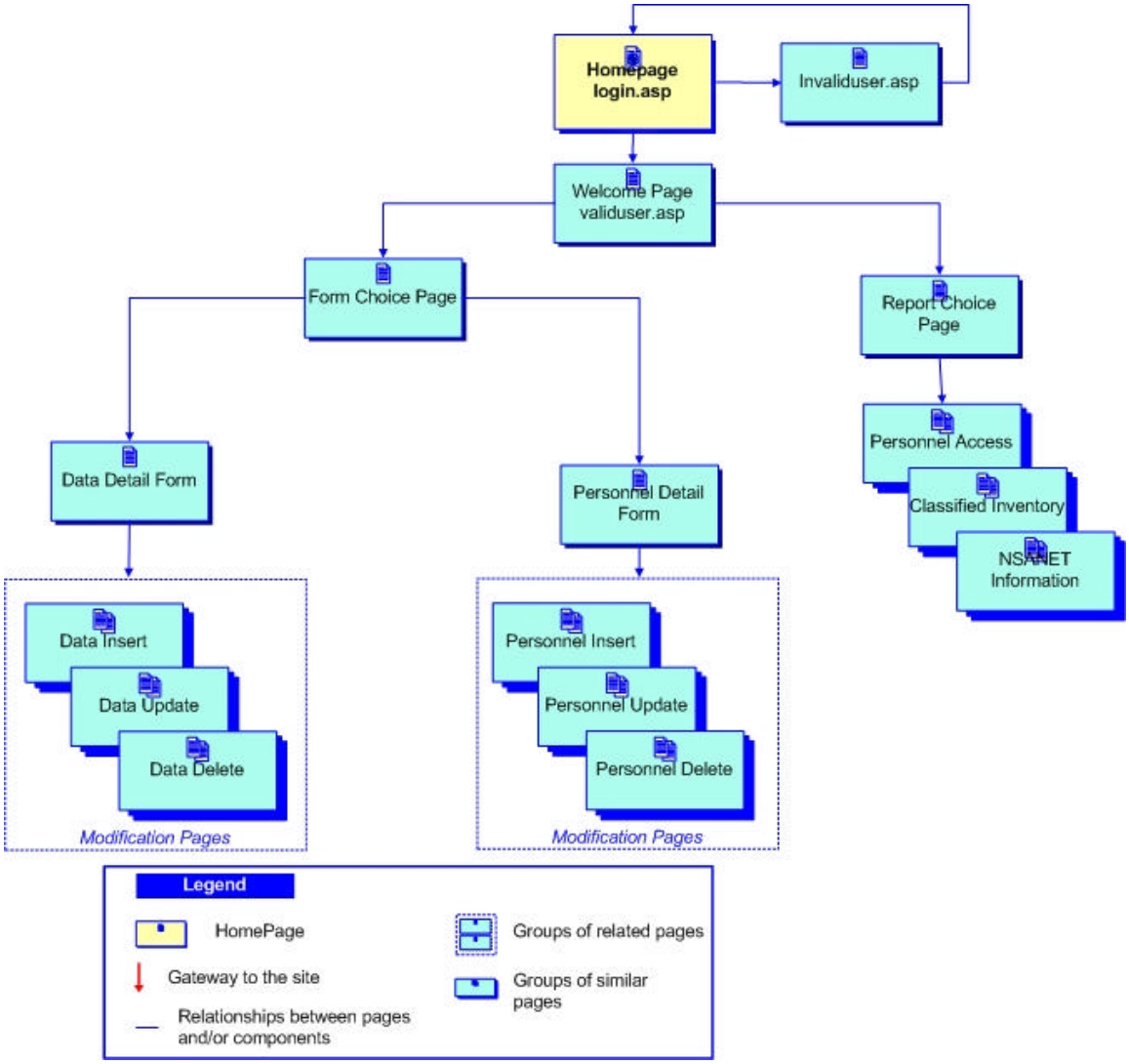


Figure 9. SCIF Website Conceptual design

1. Login Page

All users will be able to access the SCIF Web Page by typing in http://<servername>/scifdb or the Internet Protocol (IP) address of the machine that hosts the SCIF website. The user will be asked to login using their username and password.

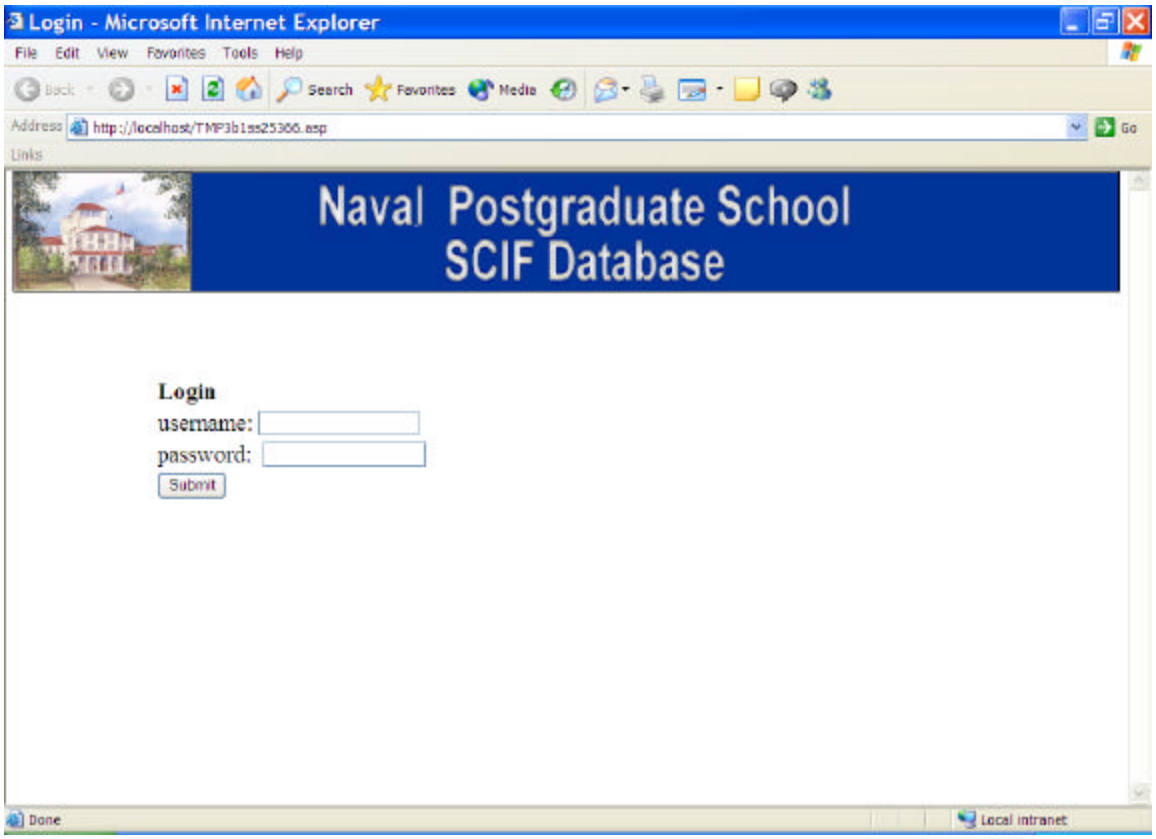


Figure 10. Login Page

2. Homepage

The SCIF homepage, Figure 11, utilizes the Windows naming convention for homepages and was created using the name index.htm in Dreamweaver MX. It was created using

frames. The use of frames allows the user to continuously view the homepage while using the center frame to display user selected data. The picture below shows the SCIF homepage. The homepage top frame contains a picture of Herman Hall and Fireworks text graphics. The left frame contains a description of the site and gives the user the choice to view either forms or reports.

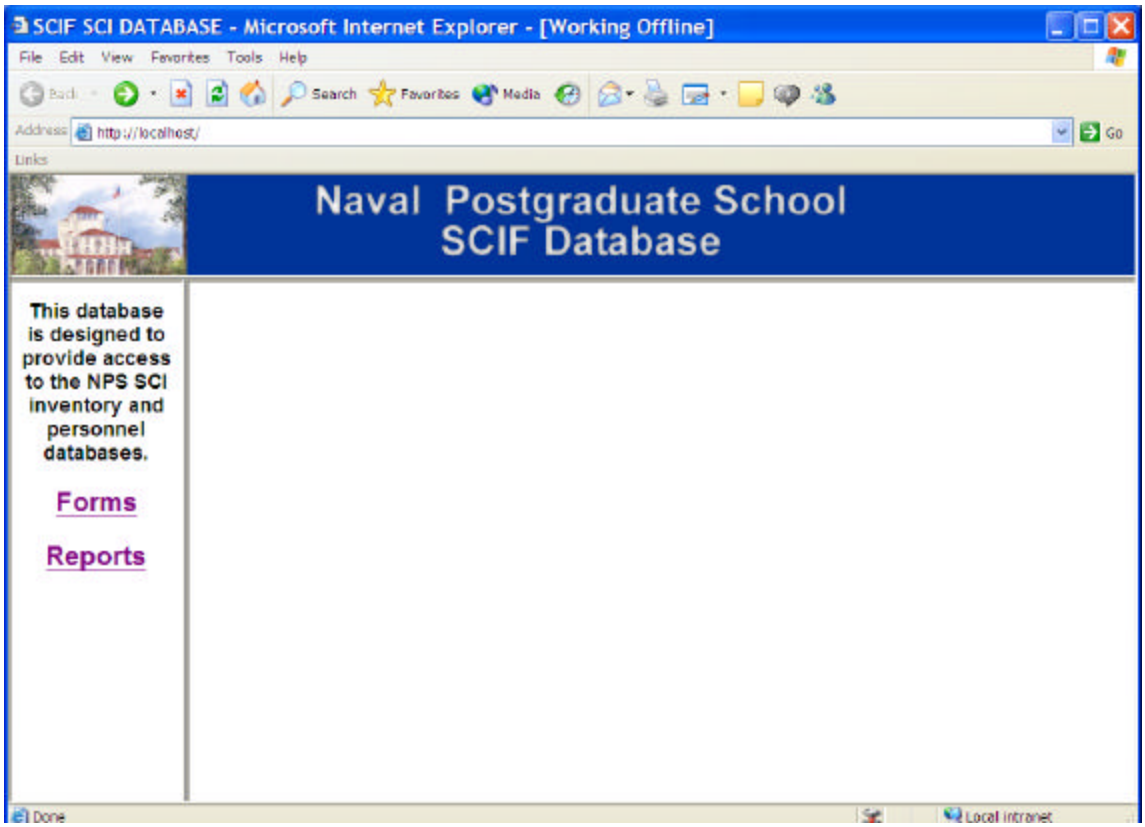


Figure 11. SCIF homepage

3. Form Choice Page

The Form Choice page, Figure 12, is named formchoice.htm. From the homepage you are able to select

Forms or Reports. The page below shows the choice if FORMS in the left frame is selected. The center frame gives the user two view choices; Data Detail Form or Personnel Detail Form.

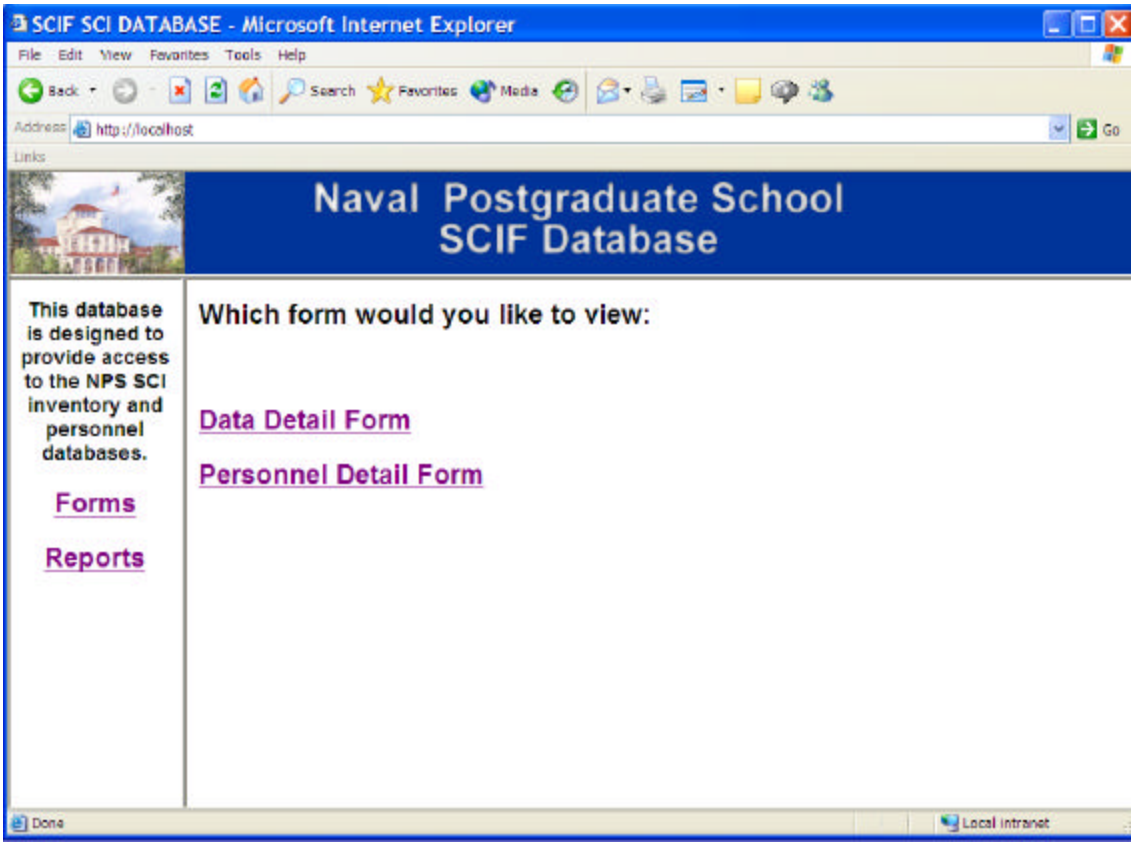


Figure 12. Form Choice Page

4. Data Detail Page

The data detail form is shown in Figure 13. The user can use the navigation buttons to scroll through the SCIF library using this page. Providing that the user has administrator or limited administrator access they will be

able to update, insert or delete data pertinent to the SCIF library holdings.

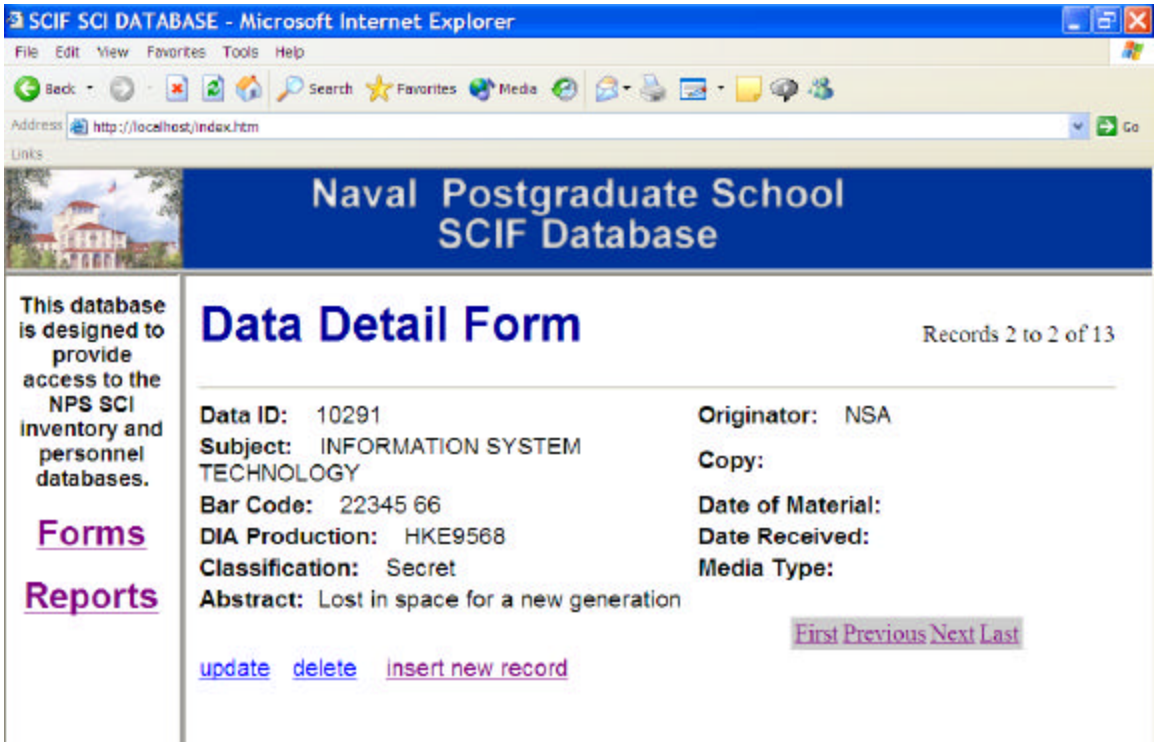


Figure 13. Data Detail Page

5. Data Insert Page

The Data Insert Form, shown in Figure 14, and the Data Update Form are virtually the same. They differ only in the information present when the form is opened; the update form will contain data on the selected item while the insert form will be blank. The update page will be receiving the Data ID number from the Detail Page so that the user can update the associated record. Only administrator or limited administrators can insert or update these forms.

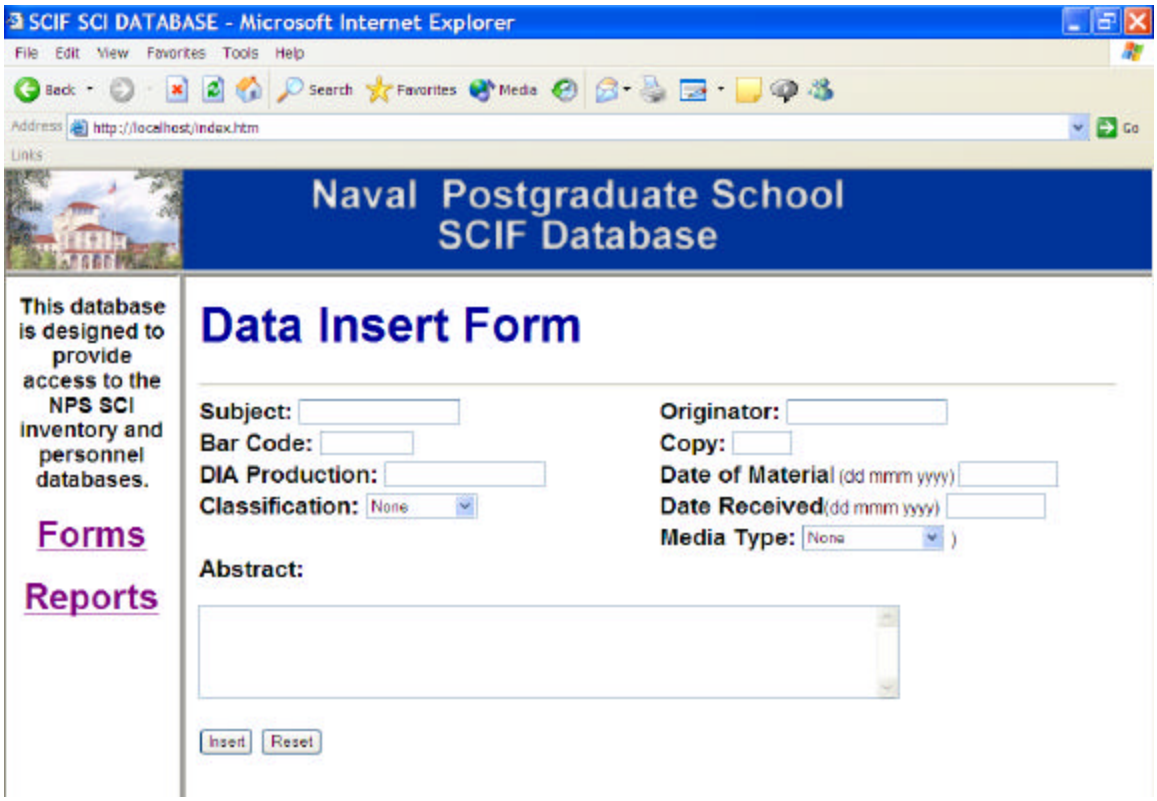


Figure 14. Data Insert Form

6. Data Delete Page

The data delete page is shown in Figure 15. A record is deleted by simply clicking the delete button near the bottom of the form.

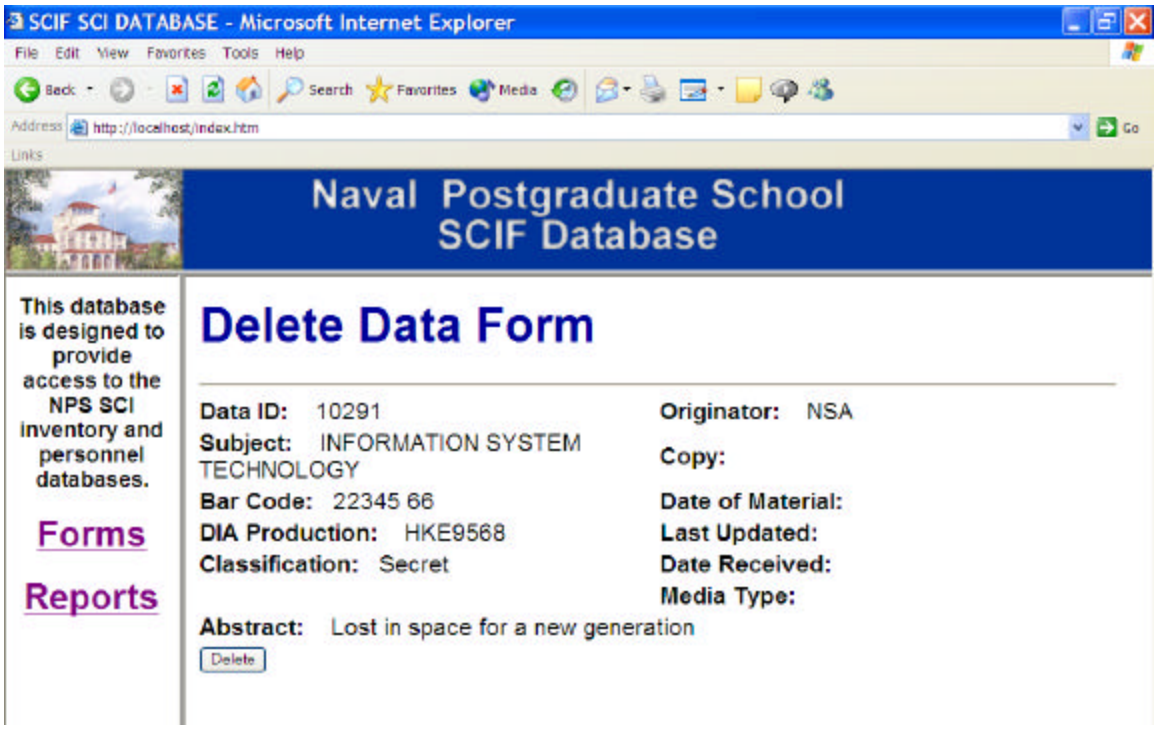


Figure 15. Data Delete Form

7. Personnel Detail Form

The Personnel Detail Form is shown in Figure 16. The user can use the navigation buttons to scroll through the personnel database using this page. Providing that the user has administrator or limited administrator access they will be able to update, insert or delete data.

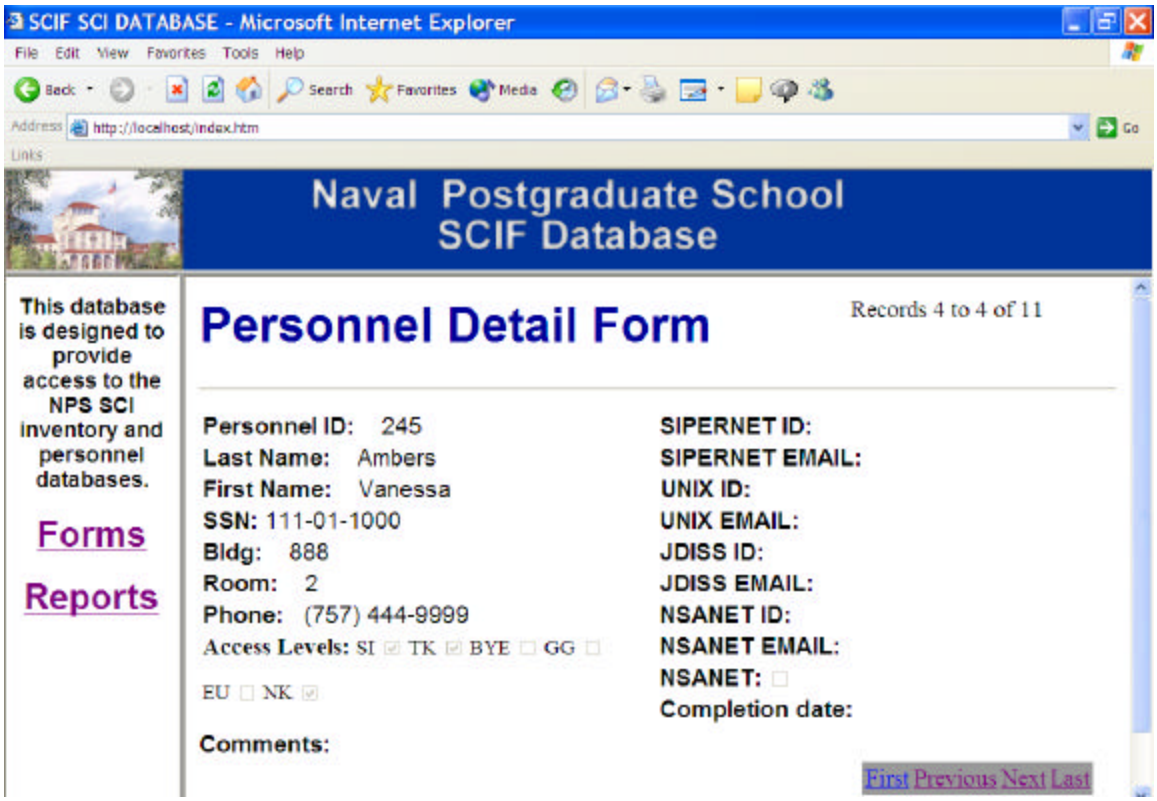


Figure 16. Personnel Detail Form

8. Personnel Update Form

The Personnel Insert Form and the Personnel Update Form, shown in Figure 17, are virtually the same. They differ only in the information present when the form is opened; the update form will contain data on the selected person while the insert form will be blank. Only administrator or limited administrators can insert or update this form.

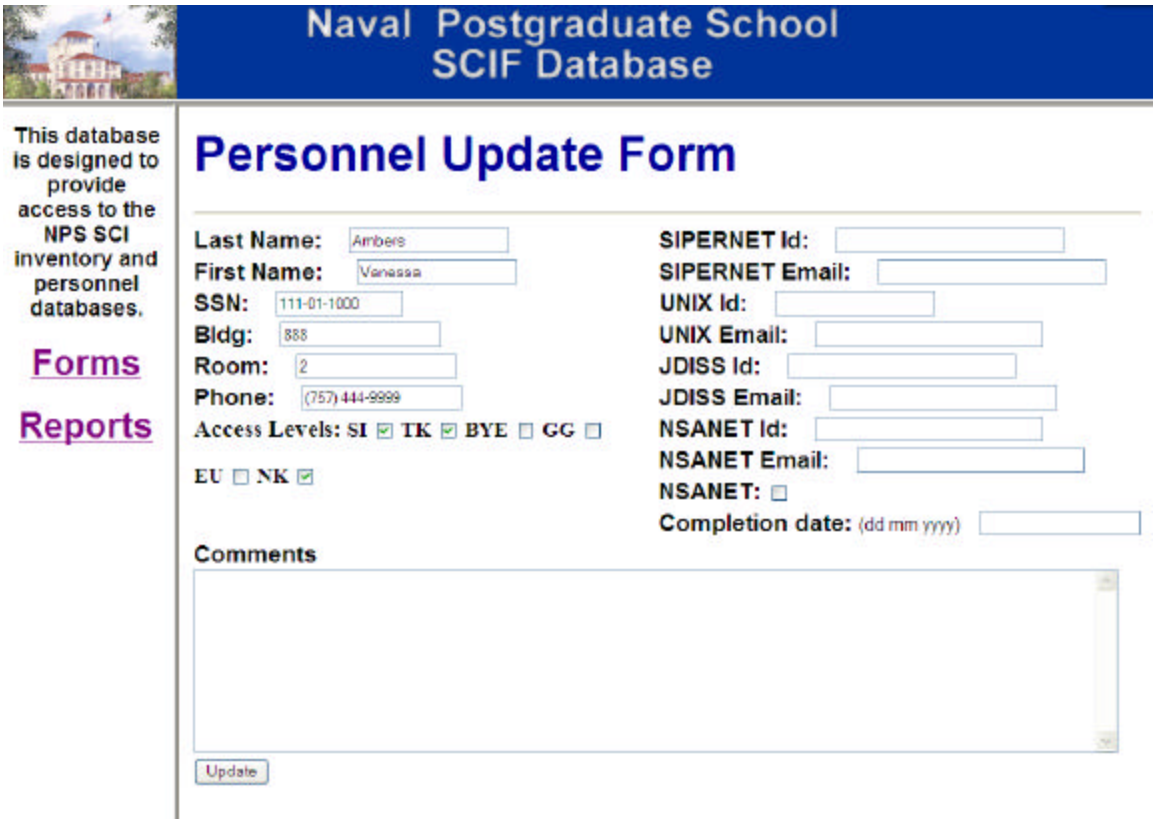


Figure 17. Personnel Update Form

9. Personnel Delete Form

The Personnel Delete Form, shown in Figure 18, allows limited administrators and administrators to delete personnel information from the database.

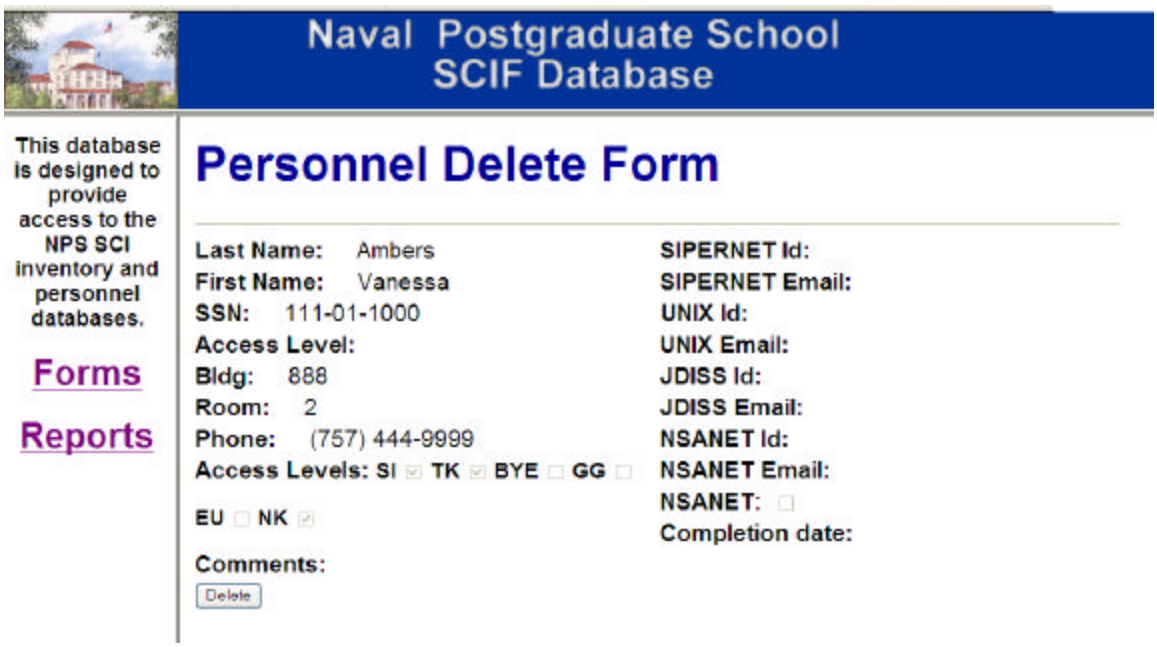


Figure 18. Personnel Delete Form

C. DREAMWEAVER USER SECURITY

Control to the SCIF database is enabled using Dreamweaver MX user authentication. A dynamic web site allows access control of editing and viewing privileges by authorized users. [5] Authentication is accomplished by adding username, password and access level fields to the Access database. Access levels assigned to each page will govern users' access to the web pages in the site. The SCIF database will have four levels of security embedded in the program.

1. Administrator Group

The first level will be an administrator level. The administrator will be allowed read, insert, modify and delete all personnel and data. Additionally, the administrator will have the ability to change the database schema. The administrator will have access to the database via the database file and the web. The Microsoft Access program will be used to make any database schema changes, append destroyed data and transfer custody of classified documents to personnel.

2. Limited Administrator

The limited administrator will be allowed to read, insert, modify and delete all personnel and data records. The limited administrator will access the database by logging on via the web interface. A limited administrator will be able to transfer custody of classified documents to personnel.

3. Extended User

The extended user will be allowed to read and view all of the personnel and data records. The extended user will access the database by logging on via the web interface.

4. User

The normal user will only be allowed to view data records contained in the SCIF library via the web interface.

D. DREAMWEAVER SITE SECURITY

Access to each page in the SCIF website is implemented by utilizing Dreamweaver’s user authentications server behavior. Security authorizations are applied to each page in the website; this functionality will keep unauthorized users from accessing a page based on an access group stored in the database table. As detailed in the user’s manual, the administrator will be responsible for assigning usernames and passwords in the database for later recall. Table 7 shows how security is applied to each page in the database.

Page	Associated Authorization Level
Homepage	Administrator, Limited Administrator, Extended User, User
Form Choice	Administrator, Limited Administrator, Extended User, User
Report Choice	Administrator, Limited Administrator, Extended User, User
Data Detail	Administrator, Limited Administrator, Extended User, User
Data Insert	Administrator, Limited Administrator
Data Update	Administrator, Limited Administrator
Data Delete	Administrator, Limited Administrator
Personnel Detail	Administrator, Limited Administrator, Extended User, User
Personnel Insert	Administrator, Limited Administrator
Personnel Update	Administrator, Limited Administrator
Personnel Delete	Administrator, Limited Administrator

Table 7. Website Authorization Table

V. SUMMARY

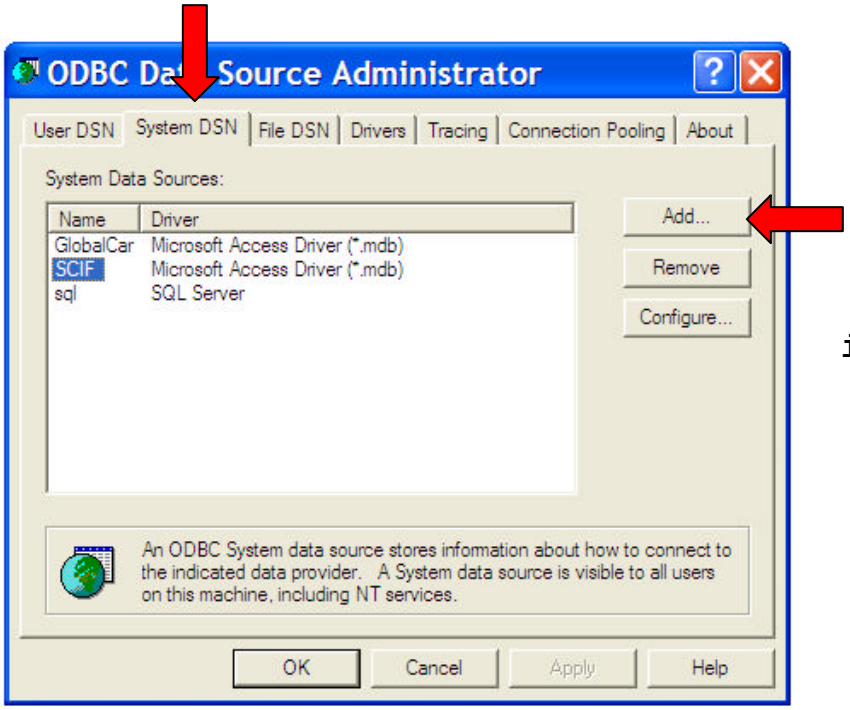
Several options were explored to determine the best method of meeting the database requirements. Since Microsoft products are in widespread use at NPS, Access 2000 was chosen as the relational database. Access 2000 also has the ability to display data via data access pages (DAPs). Research revealed that DAPs have a relatively low level of security due to limitations in protecting HTML Data Access Pages. Macromedia's Dreamweaver MX was chosen to develop the website as it provides better security by allowing the developer to assign user level authentication security feature to each page. The implementation method, detailed in this thesis, addresses the need for the consolidation of the two independent personnel and classified inventories. Additionally, it allows users to access related web pages via the Classified Intranet. By default an intranet solution provides for enhanced accessibility to the SCIF database for all users on the Intranet. As data and user demands grow, future upgrades to the database and website should be accomplished by using technologies available at NPS. There are several obstacles to take into consideration when deciding in upsizing a Microsoft database to SQL Server. Specifically, follow-on developers need to have VBScript, Visual Basic and SQL coding background prior to upgrading to a SQL server. There are features in Access that do not convert to the SQL model. For example macros, subform features and repeating drop down menus must be coded manually to duplicate existing functionality. Additionally research must be

taken to investigate potential interoperability problems between chosen technologies.

APPENDIX I ADMINISTRATOR USER MANUAL

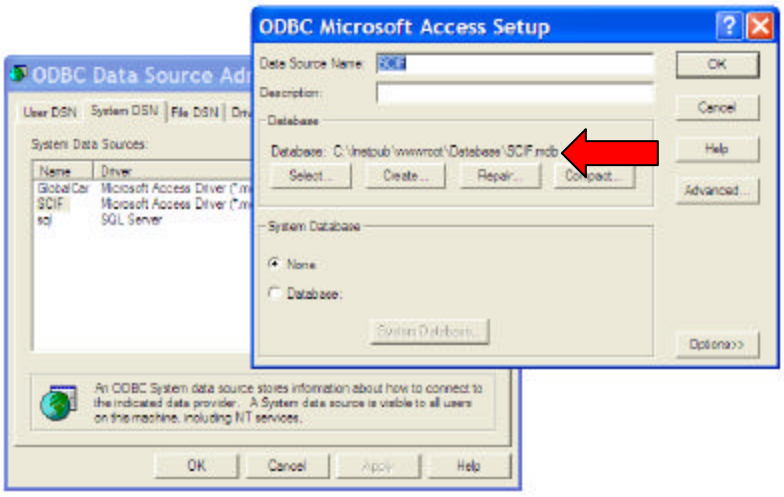
The administrator will need to routinely accomplish several tasks in maintaining the website and database.

To setup an Open Database Connection (ODBC) the administrator will click the **start** in windows and follow the path: **control panel > administrator tools > Data Sources ODBC**. Select the System DSN and ensure there is a connection named SCIF with a Microsoft Access Driver (*.mdb). If the DSN does not exist create one using the add button.



Use to add if DSN does not exist

Once the administrator presses the add button the follow screen will appear.



Select the directory the database is located in

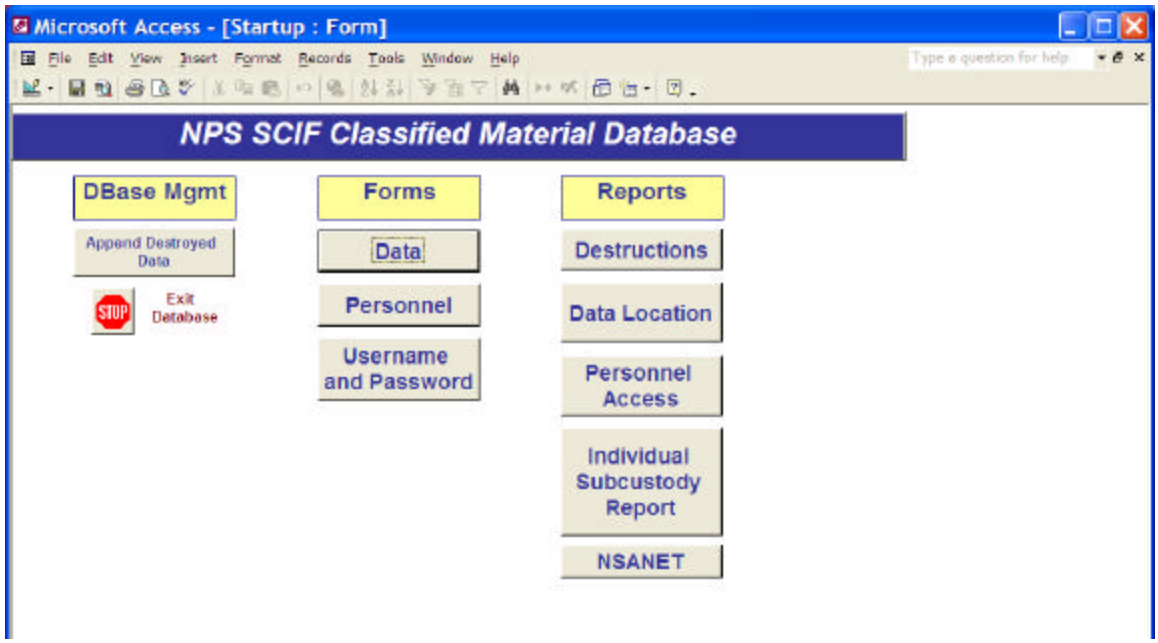
Click ok and setup is complete.

The Startup form contains three Title areas: Database Management (Dbase Mgmt), Forms and Reports. The append destroyed data action button located beneath Dbase Mgmt is used to append destroyed data information to a destroyed data table and then delete the information from the data table.

Located in the forms column are the data, personnel, and username/password action buttons. The data form is used to enter data related information. The personnel form is used to enter personnel related information. The username and password form is used to enter usernames and passwords for intranet access to the SCIF webpage. The default user level when a new person is entered into the database is user. The administrators can increase user privileges as needed using the username and password form.

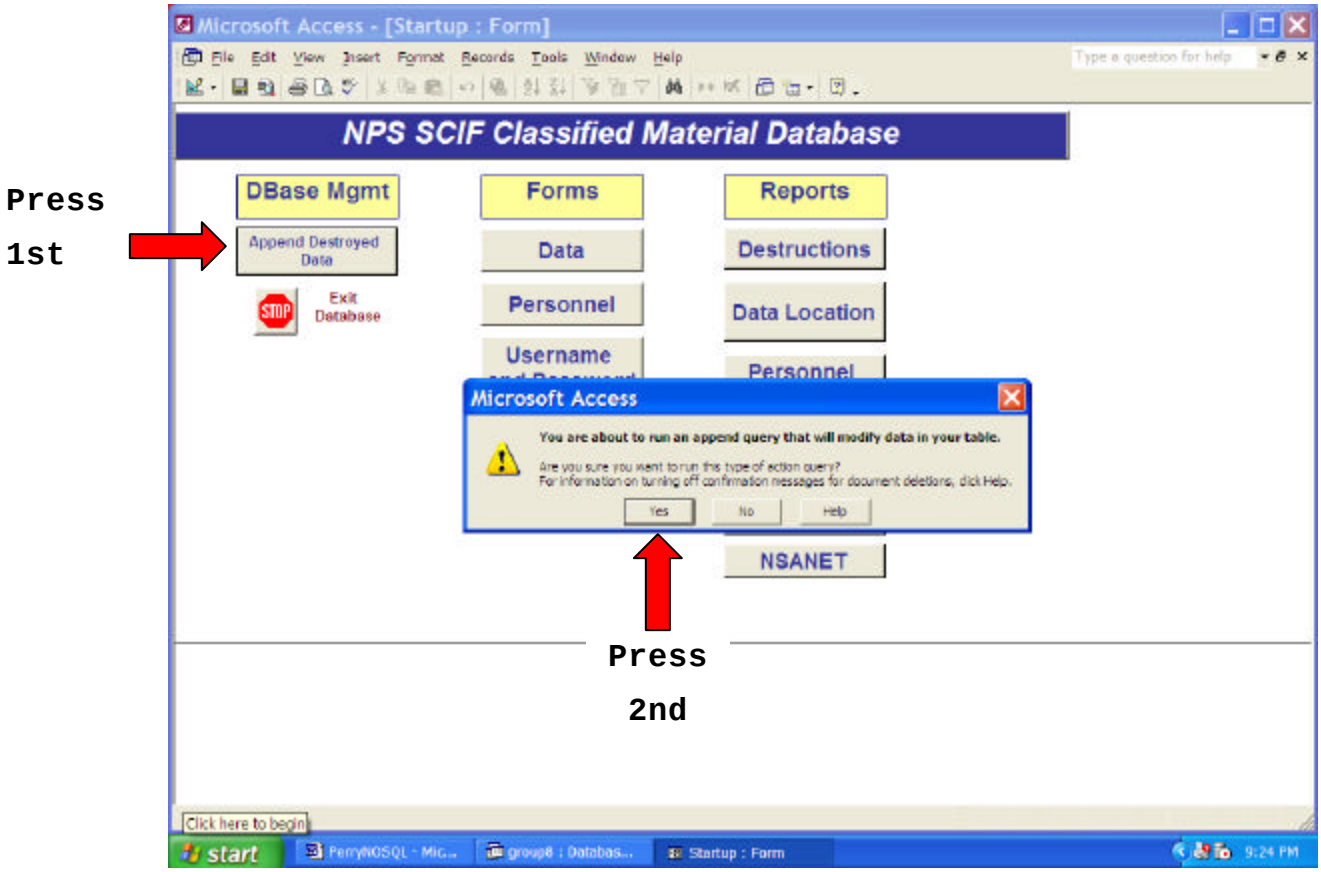
Located under the reports column are action buttons for destruction reports, data location, personnel access, individual subcustody report and NSANET reports. To print a report select desired action button.

1. Startup Form



As shown, once you click append destroyed data action button a message will indicate **"You are about to run an append query that will modify data in your table." "Are you sure you want to run this action query?"** Click **Yes** to append data from the data table to the destroyed data table. Click **No** to cancel action.

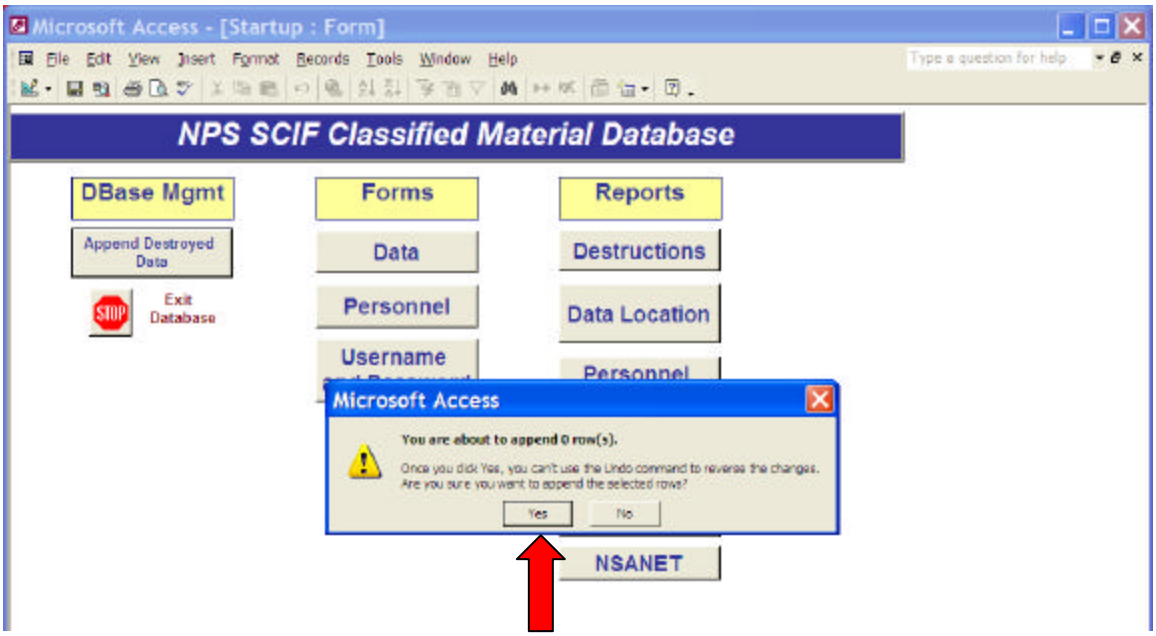
2. Append Destroyed Data



Once the user clicks **Yes**, a new Access information box will pop upon with a statement **"You are about to append # row(s). Once you click yes, you can't use the undo command to reverse the changes. Are you sure you want to append the selected rows?"** The # sign indicates the

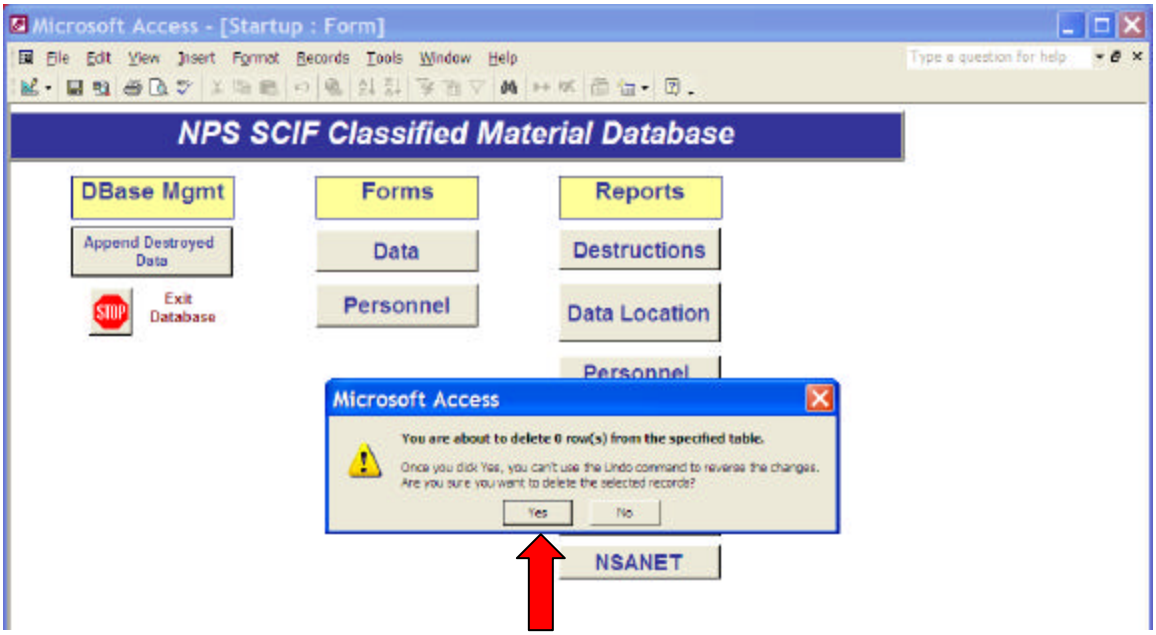
number of rows that will be appended. If the displayed statement is correct press **Yes**.

Append Destroyed Data cont.

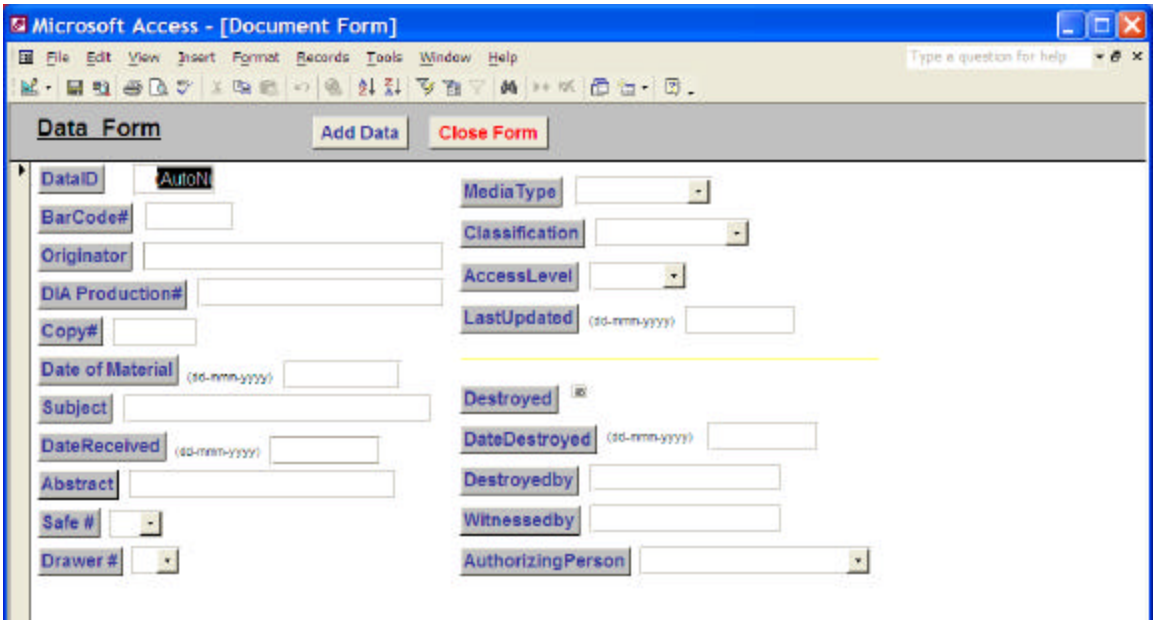


Next the delete records query will run. A message will come up that indicates. **"You are about to delete # row(s) from the specified table? Once you click yes, you can't use the undo command to reverse the changes. Are you sure you want to delete the selected records?"** Click **Yes** to delete records. Click **No** if you do not want to update you Data table by deleting destroyed data.

Append Destroyed Data cont.



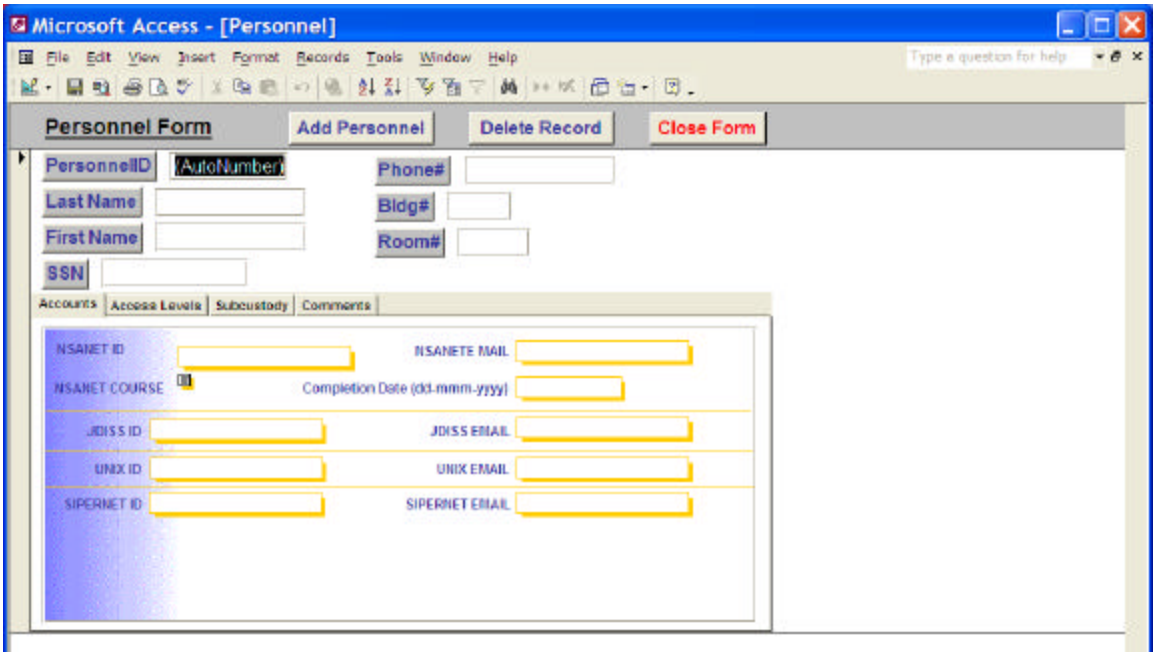
3. Enter Data



a. **DataID** - an autonumber that is generated by Access, the user cannot manipulate this number
b. **BarCode#** - enter 7 digit barcode number
c. **Originator** – enter originator name
d. **DIA Production #** - enter DIA production number
e. **Copy#** - enter copy number if applicable.
f. **Date of Material** – enter publication date of material
g. **Subject** – enter subject of material
h. **DateReceived** – enter the date received by command
i. **Abstract** – enter abstract as appropriate
j. **Safe #** - enter safe number 1 thru 24
k. **Drawer #** - enter drawer number 1 thru 4
l. **MediaType** – enter media type from the dropdown menu
m. **Classification** – enter classification from dropdown menu
n. **AccessLevel** – enter access level from dropdown menu

o. **LastUpdated** – filled in automatically from Access when data is modified
p. **Destroyed** – check box if material has been destroyed
q. **DateDestroyed** – enter the date material is destroyed
r. **Destroyedby** – enter person conducting destruction
s. **Witnessedby** – enter person witnessing destruction
t. **AuthorizingPerson** – enter person authorizing the destruction

4. Enter Personnel and Account Information



a. **PersonnelID** - is an autonumber that is generated by Access, the user cannot manipulate this number

b. **Last Name** – enter last name

c. **First Name** – enter first name

d. **SSN** – enter social security number

e. **Phone#** - enter work phone number

f. **Bldg#** - enter work building number

g. **Room#** - enter room number

h. **NSANET ID** – enter National Security Agency Network identification

i. **NSAET Email** – enter National Security Agency email address

j. **Completion Date** – enter NSA completion date

k. **JDISS ID** – enter Joint Deployable Intelligence Support System (JDISS) identification

l. **JDISS EMAIL** – enter JDISS email address

m. **UNIX ID** – enter UNIX identification

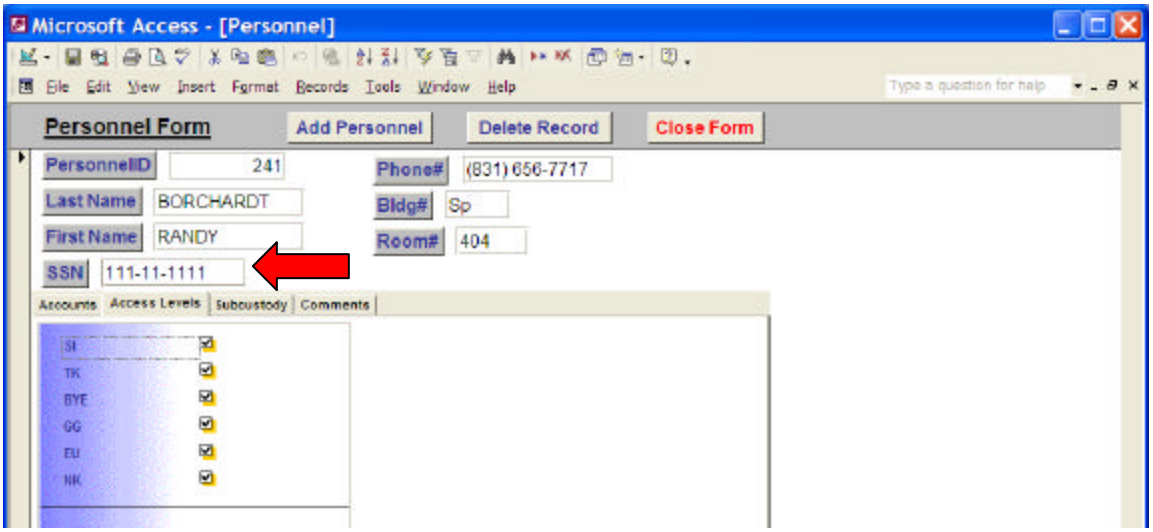
n. **UNIX EMAIL** – enter UNIX email address

o. **SIPRNET ID** – enter Secret Internet identification

p. **SIPRNET EMAIL** – enter SIPRNET email address

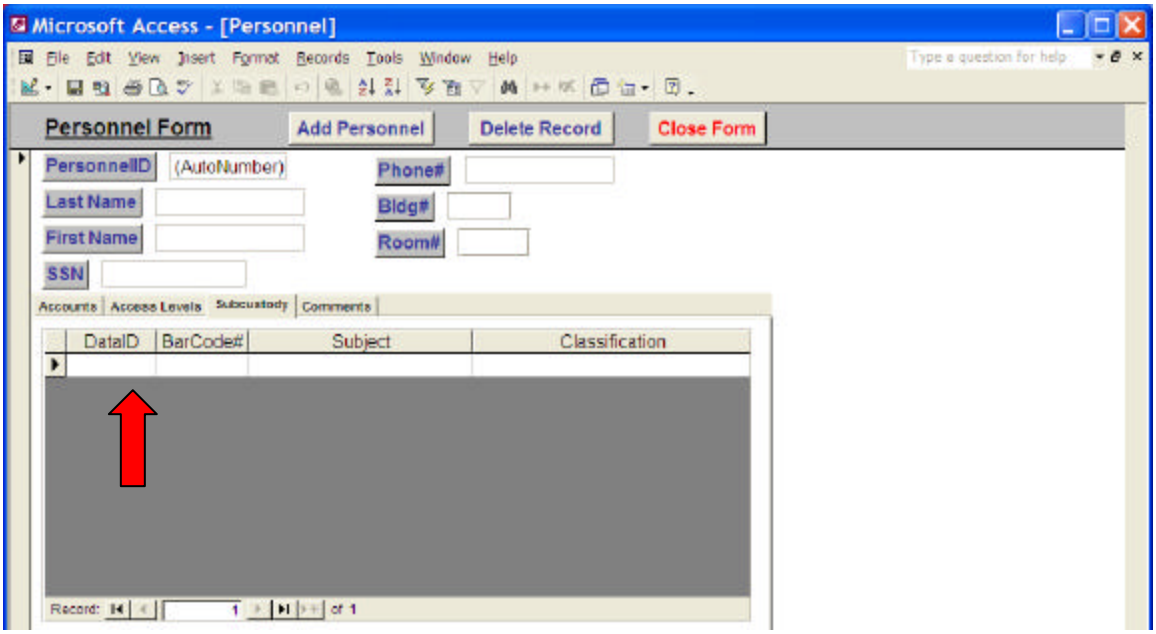
5. Enter Access Level

The Access level subform has a checkbox next to each associated access level. The user will check the boxes that correspond to the person's level of access.



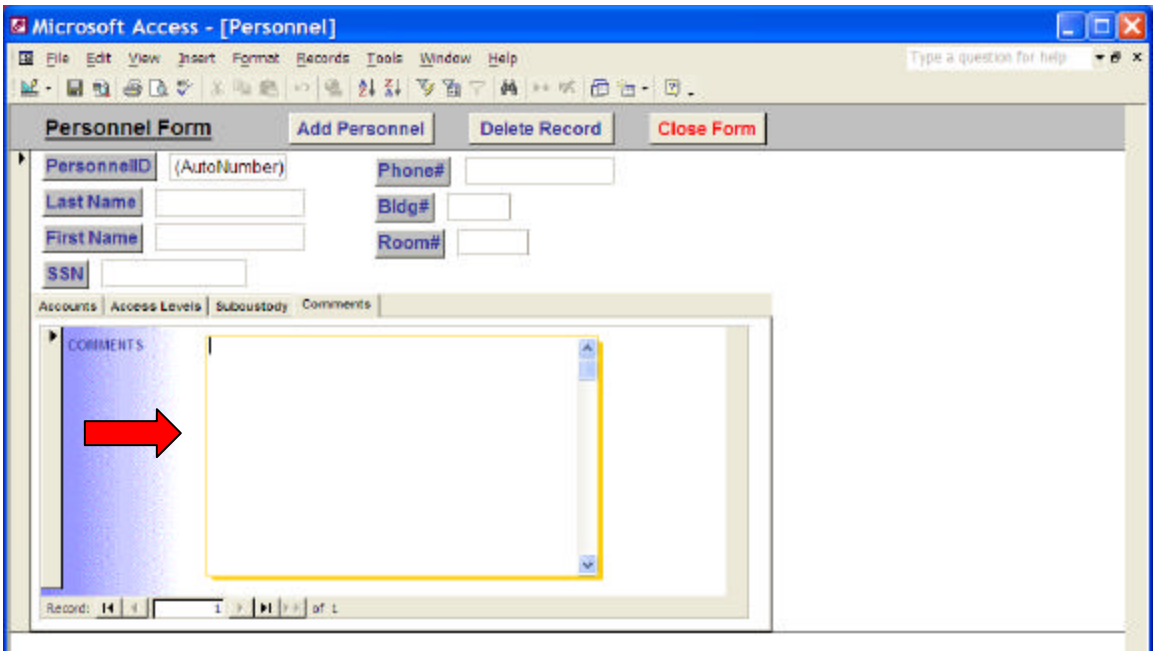
5. **Enter Subcustody information**

To transfer subcustody data to an individual the administrator will select the person to Subcustody data to. Then select the Subcustody subform and press the DataID drop down menu to select data to be assigned.



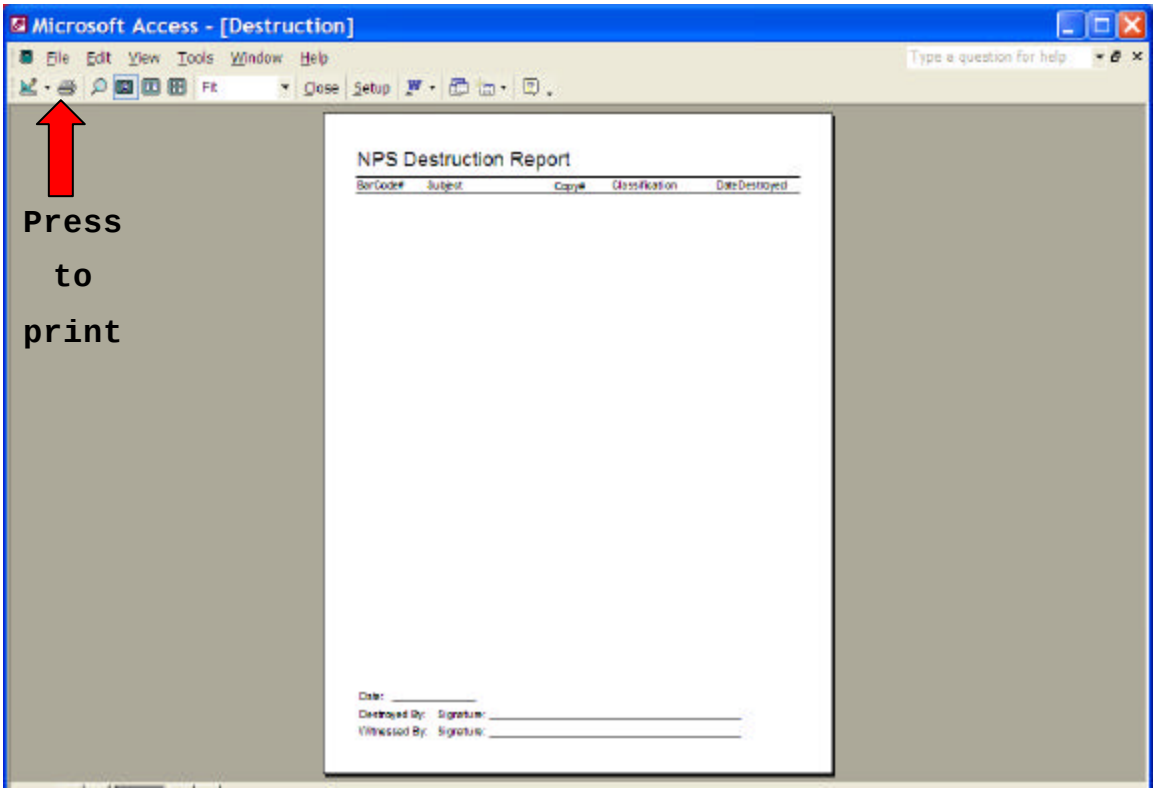
6. Comments

Comments can be entered by selecting the comments subform and enter comments as desired.



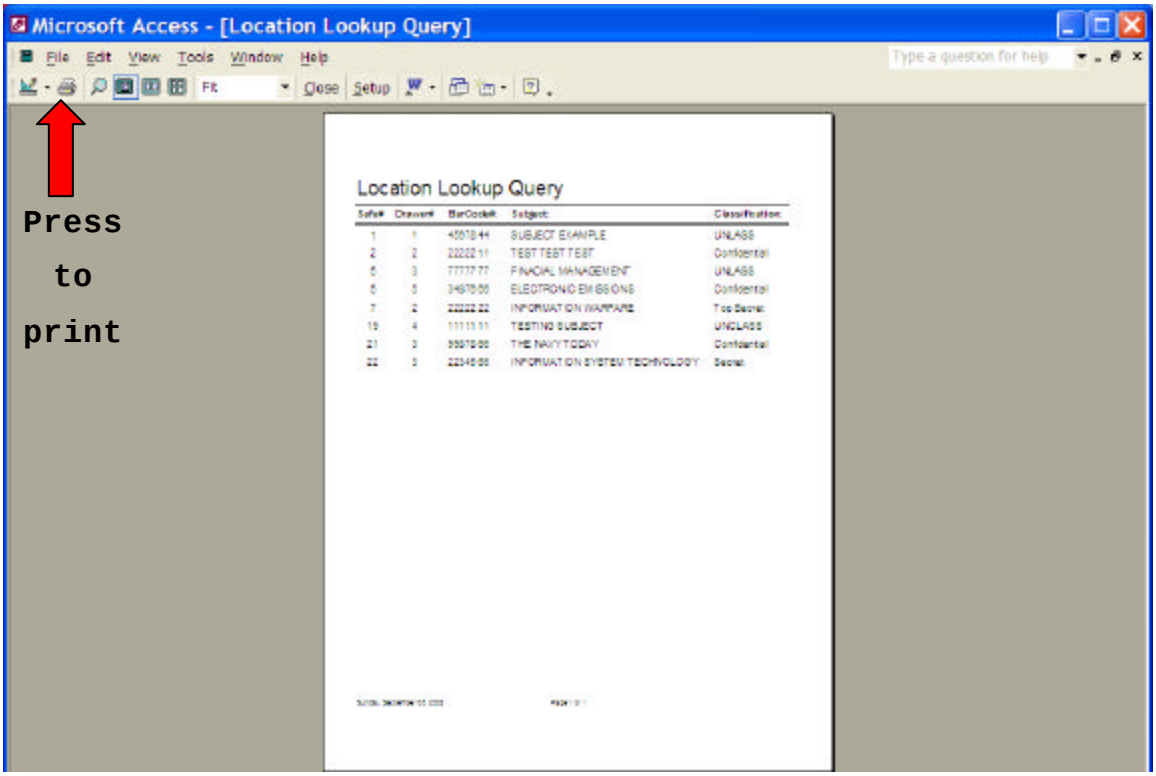
7. Print Destruction Report

This report shows data that has been destroyed. The report is formatted to display the Barcode, Subject, Copy number, classification and date of destruction. The form also has signature blocks for the people conducting and witnessing the destruction.



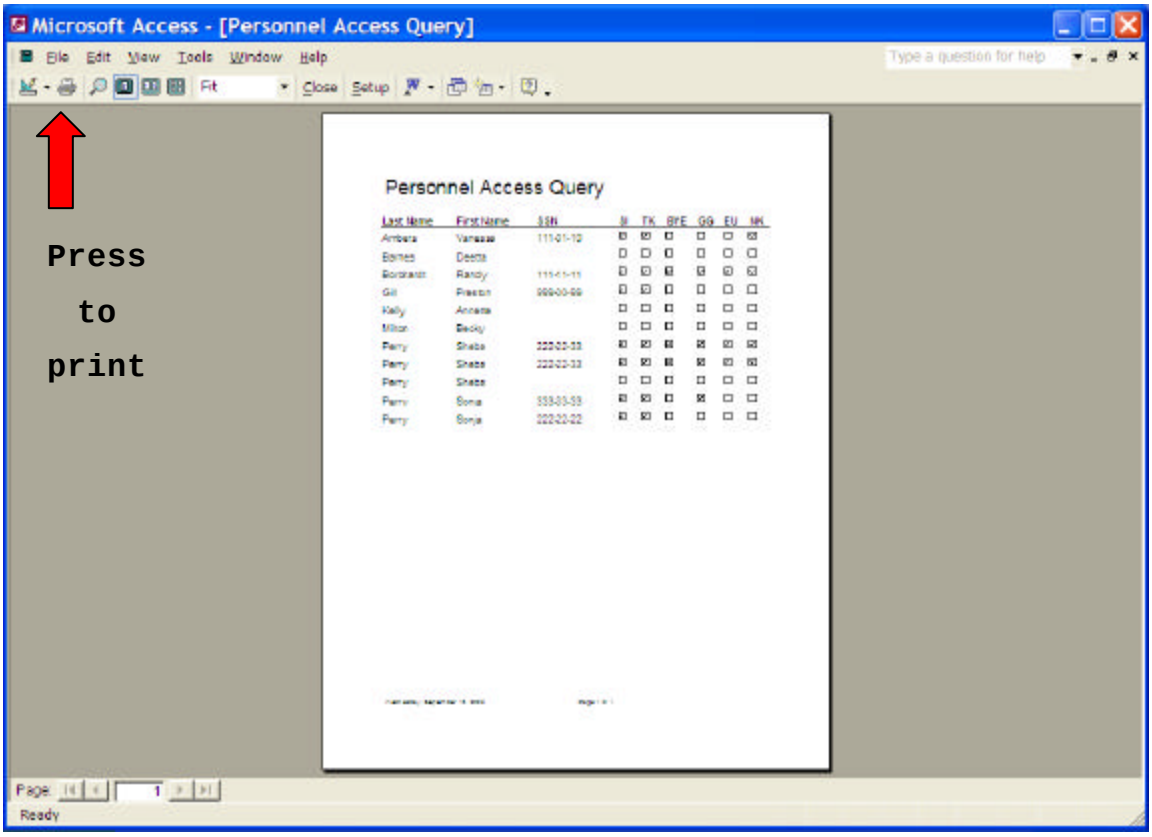
9. Print Data Location Report

The Location Report shows where each piece of data is stored. The report displays the location of data by safe number, drawer number, barcode number, subject and classification.


Microsoft Access - [Location Lookup Query]
File Edit View Tools Window Help
Close Setup
Press to print
Location Lookup Query

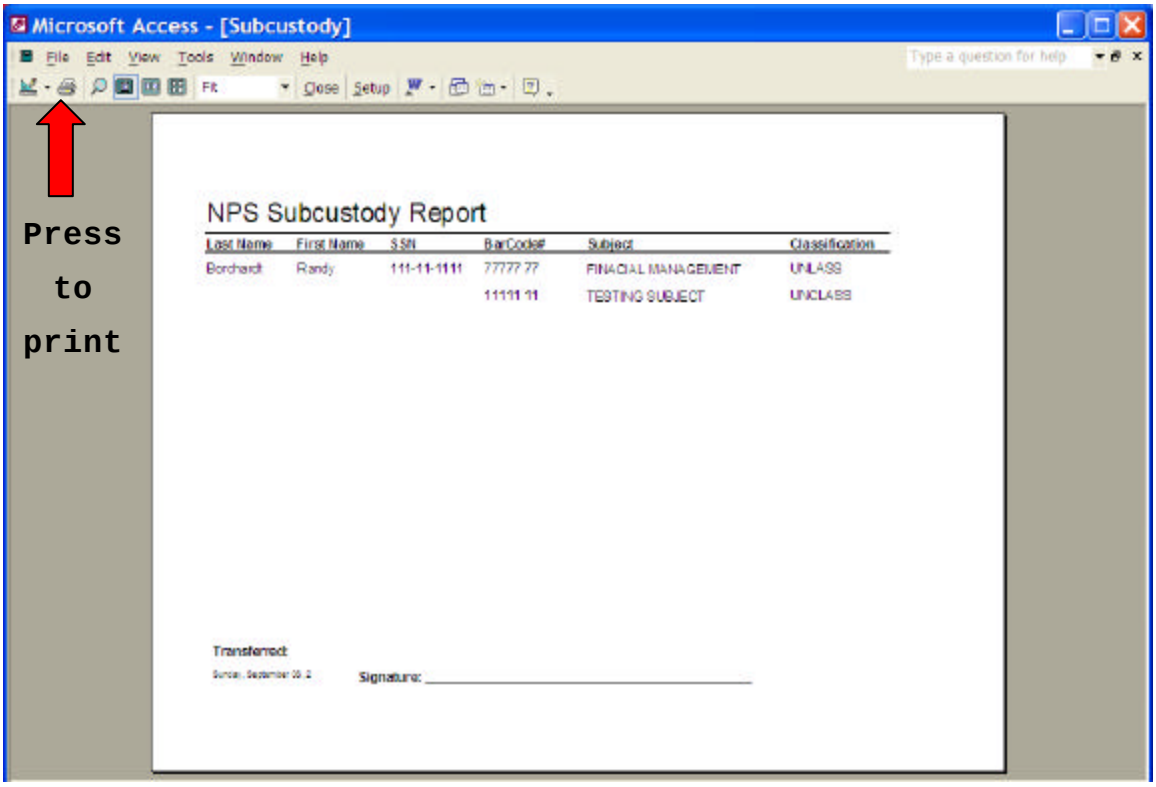
10. Print Personnel Access Report

The Personnel Access Report lists all personnel in the database along with their associated access levels.



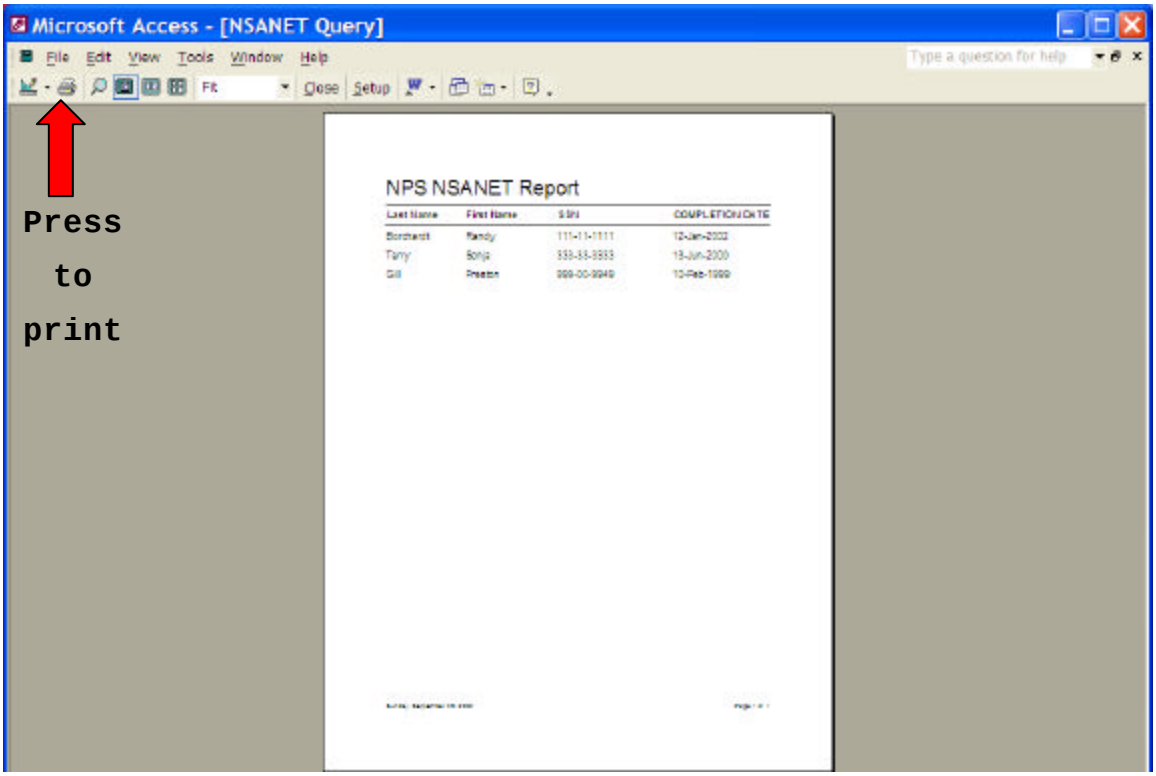
11. Print Individual Subcustody Report

The Subcustody report shows a list of all the data a person has issued to them. It lists the information by last name, first name, social security number, subject and classification.


Microsoft Access - [Subcustody]
File Edit View Tools Window Help
Close Setup
Press to print
NPS Subcustody Report
Last Name First Name SSN BarCode# Subject Classification
Borchardt Randy 111-11-1111 77777 77 FINACIAL MANAGEMENT UNLASS
11111 11 TESTING SUBJECT UNCLASS
Transferred:
Signature:

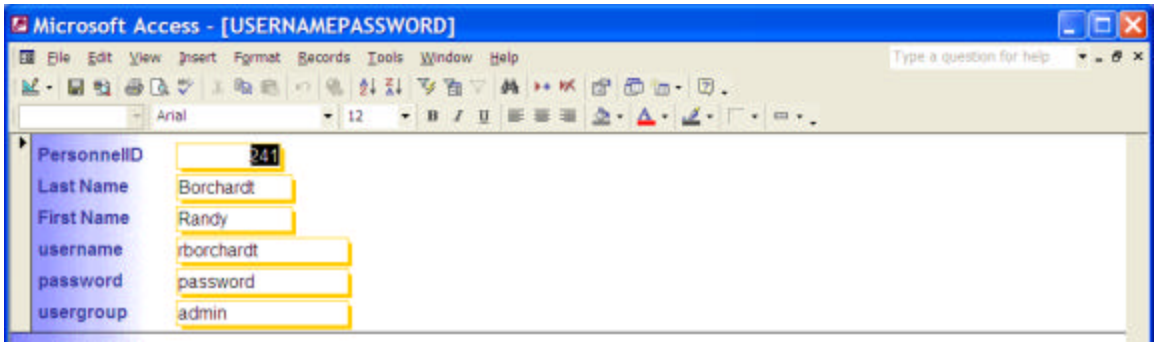
12. Print NSANET Report

This report shows all the people that have completed the NSANET course. The report displays the data by last name, first name, social security number and the date the course was completed.



13. Enter username and password

This form is used to enter username, password and usergroup fields. The PersonnelID, Last Name and First Name fields cannot be modified using this form. This form only allows modifying the username, password and usergroup.



LIST OF REFERENCES

1. Roger Jennings, *Using Microsoft Access 2000, Special Edition*, Que Corporation, 1999.

2. Kroenke, D., *Database Processing: Fundamentals, Design, Implementation,* Seventh Edition, Prentice Hall, 2000.

3. John Viescas, *Running Microsoft Access 2000,* Microsoft Press, 2000.

4. Warner, Janine & Berkowitz, Ivonne, *Dreamweaver MX,* Hungrey Minds, Inc., 2002.

5. West, Ray & Muck, Tom, *Dreamweaver UltrDev 4: A Beginner's Guide,* Osborne McGraw-Hill, 2001.

THIS PAGE INTENTIONALLY LEFT BLANK

BIBLIOGRAPHY

1. Roger Jennings, *Using Microsoft Access 2000, Special Edition*, Que Corporation, 1999.

2. Kroenke, D., *Database Processing: Fundamentals, Design, Implementation,* Seventh Edition, Prentice Hall, 2000.

3. John Viescas, *Running Microsoft Access 2000,* Microsoft Press, 2000.

4. Warner, Janine & Berkowitz, Ivonne, *Dreamweaver MX,* Hungrey Minds, Inc., 2002

5. West, Ray & Muck, Tom, *Dreamweaver UltrDev 4: A Beginner's Guide,* Osborne McGraw-Hill, 2001.

6. Microsoft Press, *Microsoft Access 2000, At a Glance,* Perspection Inc., 1999.

7. www.Microsoft.com/ql/evaluation/overview/default.asp 10 September 2002.

8. msdn.microsoft.com/library/en-us/dnapg/html/ apg01.asp?frame=true 8 January 2002.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, VA

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, CA 93943-5101

3. Randy L. Borchardt
   Naval Postgraduate School
   Monterey, CA 93943-5101

4. Sonja M. Perry
   Fleet Information Warfare Center (FIWC)
   Naval Amphibious Base
   Norfolk, VA 23521-3225

5. Dan C. Boger
   Naval Postgraduate School
   Monterey, CA 93943-5101

6. Special Security Officer
   Naval Postgraduate School
   Monterey, CA 93943-5101